WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Thursday, September 23, 2004

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L15	request with device with certificate with (set adj top)	1
☐	L14	request with device with certificate	295
		DB=USPT; PLUR=YES; OP=OR	
☐	L13	l12 and certificate with public adj key	60
		DB=PGPB,USPT,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L12	19990701	119
☐	L11	(private adj key) with (seed or (device adj identifier) or (serial adj number) or (device adj id) or (device adj serial adj number))	350
☐	L10	(set adj top) adj generat$5	4
☐	L9	19990701	65
☐	L8	(set adj top) same generat$5 same key	257
☐	L7	(set adj top) same generat$5	2777
☐	L6	19990701	53
☐	L5	(set adj top) same (public or private) same (generat$5 or produc$5)	158
☐	L4	19990701	225
		DB=USPT; PLUR=YES; OP=OR	
☐	L3	19990701	225
☐	L2	(set adj top) same (public or private)	347
☐	L1	(set adj top) near10 generat$4 near3 key$1	7

END OF SEARCH HISTORY

L Number	Hits	Search Text	DB	Time stamp
1	2	6233685.pn. and (request or devices)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:26
2	158960	device near3 (id or identification or serial or number)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:27
3	31825	device adj(id or identification or serial or number)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:28
4	31825	device adj (id or identification or serial or number)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:28
5	43	device adj (id or identification or serial or number) with public with private	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:40
6	284033	device near3 generat$5 public and private	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:41
7	105622	device adj generat$5 public and private	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:41
8	46	device adj generat$5 near3 public and private	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 18:41
9	10	(device adj generat$5 near3 public and private) and @ay<1999	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:43
10	131	device adj generat$5 same public same private	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:44
11	37	(device adj generat$5 same public same private) and @ay<1999	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 17:45
12	1403	device near3 serial adj number	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 18:42
13	0	(device near3 serial adj number) and licensing adj authorities	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 18:42
14	2	(device near3 serial adj number) and licensing adj authori$6	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/09/23 18:49

```
File 275:Gale Group Computer DB(TM) 1983-2004/Sep 23
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Sep 23
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Sep 23
         (c) 2004 The Gale Group
File  16:Gale Group PROMT(R) 1990-2004/Sep 23
         (c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2004/Sep 23
         (c)2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/Sep 20
         (c) 2004 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2004/Sep 23
         (c) 2004 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2004/Sep W2
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Aug W4
         (c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Sep 22
         (c) 2004 The Dialog Corp.
File 369:New Scientist 1994-2004/Sep W2
         (c) 2004 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2004/Sep 23
         (c) 2004 Business Wire.
File 613:PR Newswire 1999-2004/Sep 23
         (c) 2004 PR Newswire Association Inc

Set     Items   Description
S1     187294   SETTOP? ? OR SET()TOP? ? OR CONDITIONAL()ACCESS OR CABLE(1-
              W)(DEVICE? ? OR UNIT? ? OR APPARATUS?? OR MODULE? ? OR EQUIPM-
              ENT OR HARDWARE OR MACHINE OR BOX OR BOXES OR DECODER? ? OR R-
              ECEIVER? ? OR TRANSCEIVER? ? OR TERMINAL? ?)
S2     608099   (DIGITAL OR SATELLITE)()(TV OR TELEVISION)()RECEIVER? ? OR
              CABLE()(TV OR TELEVISION) OR CATV
S3      46563   PUBLIC(2W)KEY? ?
S4    2443821   CA OR CENTRAL?(1W)(AGENT? ? OR AUTHORIT??? OR AUTHORIZ? OR
              AUTHORIS?) OR CERTIF?
S5         77   S1:S2(50N)S3(50N)S4
S6         32   RD (unique items)
S7         13   S6 NOT PY=2000:2004
S8     221807   KEY???(1W)(DATA OR INFORMATION OR VALUE? ? OR NUMBER? ? OR
              PARAMETER? ? OR VARIABLE? ?) OR SEED OR RANDOM?()(NUMBER? ? OR
              NUMERAL? ? OR BIT? ? OR BYTE? ? OR DATA OR INFORMATION)
S9       1705   S4(10N)S8
S10        18   S9(50N)S3(50N)(TV OR TELEVISION OR VIDEO OR CABLE? OR DIGI-
              TAL()VTR OR VOD OR NVOD OR PROGRAM? ? OR PROGRAMMING OR BROAD-
              CAST? OR SATELLITE)
S11        13   RD (unique items)
S12        10   S11 NOT PY=2000:2004
```

7/3,K/1 **(Item 1 from file: 275)**
DIALOG(R)File 275:Gale Group Computer DB(TM)

01604909 SUPPLIER NUMBER: 14001497 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Security and privacy in a digital world.
Caruso, Denise
Digital Media, v3, n1, p6(2)
June 23, 1993
ISSN: 1056-7038 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1505 LINE COUNT: 00111

... s important for you and important for my continuing business that I don't unwittingly send you an infected product.

Public key plus DES. Because **public key** uses more computer power than DES, companies such as pay-per-view cable providers are using combination systems to perform what's called "key management." Instead of encrypting the entire movie, for example, the cable operator simply uses **public key** to encrypt the DES key that will allow you to "unlock" the channel and view the movies you paid for.

The extra authentication step isn't necessary because your key is built into your **cable decoder box** , or into a "smart card" provided to you by the cable company.

...today's credit cards, there is no personal identification tied to the transaction.

Companies like A-Squared Systems in Oakland, **CA** , and researchers such as David Chaum at the Center for Math and Computer Science at the University of Netherlands in...

7/3,K/2 **(Item 1 from file: 621)**
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02131711 Supplier Number: 55284273 (USE FORMAT 7 FOR FULLTEXT)
World's Largest Wholesale Distributor to Market ActivCard Strong Authentication Solutions.
PR Newswire, p0632
July 28, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 749

... the creation, distribution, protection and control of credentials provided for user authentication and digital signature -- static passwords, dynamic passwords and **Public Key** Infrastructure (PKI) **certificates** and keys. These services are delivered in the form of a multi-function, multi application token or smart card, or any Internet-connected device (i.e. mobile phone, **set top** box, PDA).

Corporate Wallet technology utilizes the current management infrastructure to enhance present authentication methods and support emerging security and...

7/3,K/3 **(Item 2 from file: 621)**
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01832119 Supplier Number: 54174263 (USE FORMAT 7 FOR FULLTEXT)
Deutsche Telekom and Baltimore to Integrate Security Technology.
Business Wire, p0381
March 22, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 782

... with more than 6 million mobile telephony customers. At present, 17.7 million homes are connected to Deutsche Telekom's **cable television**

network. With 10 million ISDN channels, Deutsche Telekom has more than 46.5 million telephone lines in service. With 3...

...develops and markets security products and services for a wide range of e-commerce and enterprise applications. Its products include **Public Key** Infrastructure (PKI) systems, cryptographic toolkits, security applications and hardware cryptographic devices.

Baltimore UniCERT is a modular, scalable, multipurpose **Certificate** Authority (**CA**) which issues and manages digital **certificates** for a wide range of applications including email, browsers and virtual private networks. Baltimore PKI-Plus is a developer toolkit...

7/3,K/4 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01810053 Supplier Number: 53893430 (USE FORMAT 7 FOR FULLTEXT)
PRASARA Teams With Diversinet To Provide Secure ITV Transactions.
PR Newswire, p6571
Feb 17, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 351

Diversinet Corp. is a leading provider of digital **certificate** management tools and developer of a unique **public - key** infrastructure (PKI) security authentication technology.

PRASARA will embed Diversinet's PKI technology into its e-commerce interactive television services, including...

...Out TV(R) (food delivery services). PRASARA's applications can run on any interactive television platform, and on any digital **set - top** box.

Diversinet's PKI technology obtains and verifies the validity of transactions through a single-step process.

"The efficiency and...

7/3,K/5 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01794092 Supplier Number: 53615913 (USE FORMAT 7 FOR FULLTEXT)
Diversinet Corp Announces The Hiring Of A New Vice President Of Sales.
Business Wire, p1035
Jan 22, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 437

... make tremendous gains in the marketing of our security solutions for applications like smart card authorizations, Internet services and digital **set - top** box services. We expect Mr. Ramoutar's ability, contacts and resources will be parlayed into future sales and growth for...

...the leading corporations across a broad range of industries."

Diversinet Corp. (www.dvnet.com) is a leading provider of digital **certificate** management tools and a developer of **public key** infrastructure (PKI) technology required for corporate networks, Intranets and the Internet for electronic commerce. Diversinet's proprietary PKI technology offers...

7/3,K/6 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01684562 Supplier Number: 50207074 (USE FORMAT 7 FOR FULLTEXT)

ComStream Chooses Diversinet to Deliver Secure Digital Satellite PC Card.
Business Wire, p7290061
July 29, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Newswire; Trade
Word Count: 475

... industry. Products include satellite modems and earth stations, broadcast systems, the MediaCast(TM) Satellite PC/server Receiver card, and digital **set - top** boxes.

Founded in 1984, ComStream was acquired by Spar Aerospace Limited in 1992, and is a wholly owned subsidiary. Spar is a publicly owned company based in Toronto, Canada. (www.spar. **ca**)

About Diversinet

Diversinet Corp.(www.dvnet.com) is a leading provider of Digital **Certificate** management tools and a developer of **public - key** infrastructure (PKI) technology required for corporate networks, Intranets and the Internet for electronic commerce. Diversinet's proprietary PKI technology offers...

7/3,K/7 (Item 6 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

01464016 Supplier Number: 46962667 (USE FORMAT 7 FOR FULLTEXT)
Scientific-Atlanta Introduces Explorer 2000 Digital Set-Top with Real-Time Reverse
PR Newswire, p1210ATM005
Dec 10, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1250

... architecture that permits the RISC CPU, graphics
engine, and the MPEG-2 processor to dynamically share available memory,
significantly increasing **set - top**
capabilities and affordability.
-- Scientific-Atlanta's PowerKEY(TM) digital **conditional access** system.
The PowerKEY system is the first **conditional access** (**CA**) system that
uses both **public** and private **key**
cryptography to meet security demands

of broadcast and interactive network applications. With PowerKEY **CA** ,
theft of service, falsified or denied orders, and vandalism of software
and databases can be curtailed. Sensitive information can be encrypted

and decrypted, and message content can be authenticated. The PowerKEY
system incorporates both Scientific-Atlanta technologies and **public key**

technologies from RSA Data Security, Inc., and Cylink Corporation.

-- The PowerTV(TM) Operating System, designed specifically for advanced television devices...

...into a

single package. In addition to supporting standards, these chips wi

support the PowerTV operating system and the PowerKEY **conditional access** system.

In addition to Explorer **set - tops** , Scientific-Atlanta provides most major components of an end-to-end digital broadband system, including satellite receivers, Broadband Integrated Gateways...

7/3,K/8 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04111822 Supplier Number: 54046472 (USE FORMAT 7 FOR FULLTEXT)
COMMERCENET CONSORTIUM: CommerceNet/Nielson Internet and Ecommerce Survey launches in UK.
M2 Presswire, pNA
March 8, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 955

... I/Pro, Internet Shopping Network, Netscape, Open Market SAQQARA, and Terisa Systems. CommerceNet also created and operated the first online **Public Key Certificate** Authority.

About Nielsen Media Research

Nielsen Media Research is the leading provider of media research services in the U. S. and Canada. It is the producer of the Nielsen TV ratings and the leading provider of broadcast and **cable television** information services, both nationally and locally. Through its Interactive Services division, Nielsen Media Research develops audience measurements and custom research...

7/3,K/9 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04076382 Supplier Number: 53623187 (USE FORMAT 7 FOR FULLTEXT)
RPK SECURITY: RPK Security provides encryption for VPN via satellite.
M2 Presswire, pNA
Jan 21, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 456

RDATE:190199

SAN FRANCISCO, **CA** . -- RPK Security, Inc., a technology leader in strong and fast public key encryption, today announced an agreement with Communicado Data...

...encryption technology into Communicado's SatLink fast Internet data via satellite products.

RPK's Encryptonite Engine combines the benefits of **public key** encryption systems with the speed of secret key systems in one algorithm. Coupled with Communicado's SatLink system, RPK's...

...is easily intercepted. Therefore, strong and fast encryption is required to provide the privacy customers expect. Most existing solutions use **Conditional Access** technologies designed for subscription television, which are expensive and don't provide positive authentication of sender or receiver. RPK's Encryptonite Engine provides both encryption and authentication. And since it is a **public key** system, it's also easy to manage.

Custom software development for the SatLink project is being done by ITCG, a...

7/3,K/10 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03999650 Supplier Number: 53140192 (USE FORMAT 7 FOR FULLTEXT)
-ID2 TECHNOLOGIES: iD2 1st Certificate Authority system provider to support Microsoft Windows Card OS.
M2 Presswire, pNA
Oct 27, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 663

... using the new Microsoft smart card operating system - the Windows Card, which was launched today.

iD2 Technologies will enhance its **Certificate** Manager product to support the Windows Card for enterprise solutions and large scale public applications. iD2 will develop new PKI (**Public Key** Infrastructure) functionality and features for Microsoft's card components and applications.

Bjorn Gustavsson, president of iD2 Technologies, said: "The launch...

...Windows Card by Microsoft further ensures that smart card technology is the future standard for security on the Internet. PCs, **set - top** boxes, mobile phones and other digital devices are now being equipped with smart card reading facilities as standard opening the...

7/3,K/11 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

03783351 Supplier Number: 45383982
High-performance encryption chip from VLSI to ship by fall
InfoWorld, p48
March 6, 1995
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:
VLSI Technology Inc, based in San Jose, **CA** , plans to start shipping the VL06868, its high-performance encryption chip, by the fall of 1995. The chip is expected to find use in CD-ROMs, cellular telephones, information delivery systems, **set - top** boxes, smart cards, and wireless networks. The VL06868 is expected to be embedded in various hardware and software platforms, including the Information Vending Encryption System (IVES) by American Tel & Tel. The chip uses Diffie-Hellman-based **public key** encryption. ...

7/3,K/12 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10589876 SUPPLIER NUMBER: 53173826 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Tomorrow Begins Today at Net Security Firm.
American Banker, 163, 211, NA
Nov 3, 1998
ISSN: 0002-7561 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1533 LINE COUNT: 00122

... both and likes what they are doing in software and browser products to incorporate, and further the cause of, digital **certificates** . Meanwhile, it is cheering computer-keyboard, **set - top** box, and hand-held-device manufacturers for beginning to build in smart card readers.

Verisign Inc., a Silicon Valley neighbor, and Entrust Technologies Inc., a Richardson, Tex., spinoff of Northern Telecom of Canada, blazed the

certification industry's trail to the initial public offering market this year. Spyrus crosses paths with them and hopes to better...

...I applaud them," said Ms. Pontius.

"We are out to accelerate the marketplace-we need Entrust and Verisign and more" **certificate** authorities, Ms. Pontius said. "With multiple products, the best of breed will win. How many **public key** smart cards are there today? Entrust and Verisign's revenues are minuscule compared to what this industry is going to...

7/3,K/13 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire

00060265 19990615166B0392 (USE FORMAT 7 FOR FULLTEXT)
New Entrust-Ready Solutions, Technology Achievements and Business Relationships Announced at Entrust SecureSummit '99
Business Wire
Tuesday, June 15, 1999 09:36 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,469

...Organizations using Entrust's e-business solutions will have the option to benefit from nCipher's nFast/KM and nFast/ **CA** hardware key management solutions whichprotect sensitive cryptographic keys in Federally- **certified** tamper-resistant hardware, and accelerate digital signatures by offloading cryptographic processing from host server to a dedicated peripheral. http://www.ncipher.com

- NDS Americas, Inc.: The leading provider of **conditional access** technology for Pay TV, has joined the new Entrust Alliance Developer Program. The NDS AccessGear(TM) system for smart card based network security will undergo functionality testing with Entrust to offer secure **public - key** smart cards and management solutions for enterprises deploying Entrust/PKI(TM). http://www.ndsworld.com

```
File 348:EUROPEAN PATENTS 1978-2004/Sep W02
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040916,UT=20040909
         (c) 2004 WIPO/Univentio

Set     Items   Description
S1      15513   SETTOP? ? OR SET()TOP? ? OR CONDITIONAL()ACCESS OR CABLE(1-
             W)(DEVICE? ? OR UNIT? ? OR APPARATUS?? OR MODULE? ? OR EQUIPM-
             ENT OR HARDWARE OR MACHINE OR BOX OR BOXES OR DECODER? ? OR R-
             ECEIVER? ? OR TRANSCEIVER? ? OR TERMINAL? ?)
S2       9722   (DIGITAL OR SATELLITE)()(TV OR TELEVISION)()RECEIVER? ? OR
             CABLE()(TV OR TELEVISION) OR CATV
S3       7231   PUBLIC(2W)KEY? ?
S4     317914   CA OR CENTRAL?(1W)(AGENT? ? OR AUTHORIT??? OR AUTHORIZ? OR
             AUTHORIS?) OR CERTIF?
S5         62   S1:S2(50N)S3(50N)S4
S6         48   S5 AND AC=US/PR
S7         40   S6 AND AY=(1970:1999)/PR
S8         31   S5 AND PY=1970:1999
S9         45   S7:S8
S10     64673   KEY???(1W)(DATA OR INFORMATION OR VALUE? ? OR NUMBER? ? OR
             PARAMETER? ?) OR SEED OR RANDOM?()(NUMBER? ? OR NUMERAL? ? OR
             BIT? ? OR BYTE? ? OR DATA OR INFORMATION)
S11       347   S4(10N)S10(10N)S3
S12        33   S11(50N)(TV OR TELEVISION OR VIDEO OR CABLE? OR DIGITAL()V-
             TR OR VOD OR NVOD OR PROGRAM? ? OR PROGRAMMING OR BROADCAST? -
             OR SATELLITE)
S13        32   S12 NOT S9
S14        13   S13 AND AC=US/PR
S15         6   S14 AND AY=(1970:1999)/PR
S16         5   S13 AND PY=1970:1999
S17         8   S15:S16
```

9/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01406013
Source authentication of download information in a conditional access system
Quellenauthentifizierung von Datenfernladungsinformation in einem System mit bedingtem Zugang
Authentification de la source d'informations telechargees dans un systeme a acces conditionnel
PATENT ASSIGNEE:
Scientific Atlanta, Inc., (2270201), Intellectual Property Department (ATL 4.3.), 5030 Sugarloaf Parkway, Lawrenceville, Georgia 30044, (US), (Applicant designated States: all)
INVENTOR:
Akins, Glendon L., III, 2713 Beaver Ct,, Fort Collins, CO 80526, (US)
Banker, Robert O., 1581 Chamblee Gap Road, Cumming, GA 30040, (US)
Palgon, Michael S., 1196 Poplar Grove Drive, Atlanta, GA 30306, (US)
Pinder, Howard G., 4317 Stilson Circle, Norcross, GA 30092, (US)
Wasilewski, Anthony J., 10680 Wren Ridge Road, Alpharetta, GA 30022, (US)
LEGAL REPRESENTATIVE:
Holmes, Miles Keeton et al (72832), Novagraaf SA 25, Avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)
PATENT (CC, No, Kind, Date): EP 1189439 A2 020320 (Basic)
APPLICATION (CC, No, Date): EP 2001126558 980731;
PRIORITY (CC, No, Date): US 54575 P 970801; US 127152 980731
DESIGNATED STATES: DE; FR; GB; IT; NL
RELATED PARENT NUMBER(S) - PN (AN):
EP 1013091 (EP 98939155)
INTERNATIONAL PATENT CLASS: H04N-007/16; H04N-007/167
ABSTRACT WORD COUNT: 102
NOTE:
Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200212	996
SPEC A	(English)	200212	28351
Total word count - document A			29347
Total word count - document B			0
Total word count - documents A + B			29347

...SPECIFICATION to MUX 200 encapsulated in EMM 111.
MSK 208 and other parts of EMM 111 are preferably encrypted using a **public key** algorithm, such as the well-known RSA algorithm, with a **public key** associated with the specific **set - top** box 113 to which the EMM is addressed. The **public keys** of all **set - top** boxes 113 in a system 101 are stored in **Public Key** Data Base 207. The **public keys** in this data base are preferably **certified** by a **certificate** authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In...
unit(underscore)message 1011 will be examined in more detail later.

EMM Structure Details: FIG. 11
FIG. 11 shows a **CA** message 805 which contains an EMM 1112. CA message 805 has a header 1003, a CA EMM message 1101, and...

...information from the EMM(underscore)inside(underscore)header. This information is particularly sensitive and is consequently encrypted by both the **public key** of DHCT 333, for privacy reasons, and the private key of the entitlement agent or the **conditional access** authority, to apply a digital signature. Upon reception, and after the privacy decryption, if the signature verification fails, the EMM is discarded by DHCT 333. Included in this information are an ID for the **conditional access** system, the type of the CA message, the serial number of the microprocessor in the DHCT's DHCTSE 627, an identifier for the CAA or EA

a processor for performing a secure hash...

...control word; and
a transmission device for transmitting said source authentication token, said control word, and said download information;
a **set top** terminal for verifying an information source, said **set top** terminal comprising:
a port for receiving a message comprising said download information, said source authentication token, and said control word from said entitlement agent;
a memory for storing a **public key** that is included in said **public** -private **key** pair;
a decryptor coupled to said port for decrypting said control word using said **public key** ;
a processor coupled to said decryptor for performing a secure hash function having as inputs said control word and said...

...download information as authentic when the two are the same; and
a communication medium for coupling said certification authority, said **set top** terminal; and said entitlement agent.
11. The **cable television** system of claim 10, wherein said entitlement agent can authenticate different types of download information.
12. The cable television system...

9/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01406012
Method and apparatus for geographically limiting service in a conditional access system
Vorrichtung und Verfahren zur geographischen Dienstbeschrankung in einem System mit bedingtem Zugang
Procede et appareil permettant de limiter geographiquement les services dans un systeme a acces conditionnel
PATENT ASSIGNEE:
Scientific Atlanta, Inc., (2270201), Intellectual Property Department (ATL 4.3.), 5030 Sugarloaf Parkway, Lawrenceville, Georgia 30044, (US), (Applicant designated States: all)
INVENTOR:
Akins, Glendon L., III, 2713 Beaver Ct., Fort Collins, CO 80526, (US)
Wasilewski, Anthony J., 10680 Wren Ridge Road, Alpharetta, GA 30022, (US)
Pinder, Howard G., 4317 Stilson Circle, Norcross, GA 30092, (US)
LEGAL REPRESENTATIVE:
Holmes, Miles Keeton et al (72832), Novagraaf SA 25, Avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)
PATENT (CC, No, Kind, Date): EP 1189438 A2 020320 (Basic)
APPLICATION (CC, No, Date): EP 2001126557 980731;
PRIORITY (CC, No, Date): US 54575 P 970801; US 127273 980731
DESIGNATED STATES: DE; FR; GB; IT; NL
RELATED PARENT NUMBER(S) - PN (AN):
EP 1010325 (EP 98938225)
INTERNATIONAL PATENT CLASS: H04N-007/16; H04N-007/167
ABSTRACT WORD COUNT: 102
NOTE:
Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200212	1385
SPEC A	(English)	200212	28346
Total word count - document A			29731
Total word count - document B			0
Total word count - documents A + B			29731

...SPECIFICATION to MUX 200 encapsulated in EMM 111.

The geo-political **CA certificate** 2807 shown in FIG. 28, is not required to operate the normal **conditional access** and electronic activities ...of the operator's DBDS. In this case, the signature chains may be readily linked to those of geo-political **CA** and its signature 2807 by having the **public keys** of one or all of the DHCT root signature 2804, the Root CAA signature 2808 or operator CAA signatures 2802 **certified** by the geo-political **CA** signature. This is accomplished by having a **certificate** placed in a database for each of the public keys associated with signatures 2804, 2808 and 2802. Said certificate is...

9/3,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01302302
OBJECT SECURITY IMPLEMENTATION
DURCHFUHRUNG DER OBJEKTSICHERUNG
MISE EN OEUVRE DE LA SECURITE D'UN OBJET
PATENT ASSIGNEE:
General Instrument Corporation, (1403172), 101 Tournament Drive, Horsham, Pennsylvania 19044, (US), (Proprietor designated states: all)
INVENTOR:
EISENBART, Robert, S., 833 East J Street, Chula Vista, CA 91910, (US)
CHEN, Annie, O., 12927 Long Boat Way, Del Mar, CA 92014, (US)
MURPHY, Patrick, J., 8631 A1 Court, San Diego, CA 92123, (US)
LEGAL REPRESENTATIVE:
Bohnenberger, Johannes, Dr. (55291), Meissner, Bolte & Partner Postfach 86 06 24, 81633 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1232652 A2 020821 (Basic)
EP 1232652 B1 030514
WO 2001035670 010517
APPLICATION (CC, No, Date): EP 2000991391 001110; WO 2000US31043 001110
PRIORITY (CC, No, Date): US 165095 P 991112; US 173963 P 991230; US 493984 000128
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04N-007/24; H04N-005/00
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200320	809
CLAIMS B	(German)	200320	766
CLAIMS B	(French)	200320	865
SPEC B	(English)	200320	3602
Total word count - document A			0
Total word count - document B			6042
Total word count - documents A + B			6042

...SPECIFICATION with a user. The headend includes hardware that receives video and distributes it to the set top boxes within the **CA** system. Select set top boxes are allowed to decode certain video programs according to entitlement information sent by the cable...

...pay per view program, an entitlement message is broadcast in encrypted form to all set top boxes. Only the particular **set top** box the entitlement message is intended for can decrypt it. Inside the decrypted entitlement message is a key that will decrypt the pay per view program. With that key, the **set top** box decrypts the pay per view program as it is received in real-time. Some systems sign entitlement messages.
As described above, conventional **CA** systems only check entitlement of content upon receipt. More sophisticated techniques are always desired to further ensure against content being received from unintended sources.
WO-A-98 56180 discloses a global **conditional access** system for

broadcast services. US-A-5005200 discloses a **public key** /signature cryptosystem with enhanced digital signature **certification** .

SUMMARY OF THE INVENTION

The invention is as set out in sending method claim 1, receiving method claim 8 and system claim 14.

According to the invention, disclosed are an apparatus and methods for authenticating information sent to a **set top** box. In one embodiment, a method for distributing information that includes a signature is disclosed. In one step the signature...

9/3,K/5 (Item 5 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01145353

A COPY PROTECTION SYSTEM FOR HOME NETWORKS

KOPIERSCHUTZSYSTEM FUR HAUSNETZWERKE

SYSTEME DE PROTECTION CONTRE LA COPIE POUR RESEAUX DOMESTIQUES

PATENT ASSIGNEE:

Thomson Licensing S.A., (2880640), 46, quai Alphonse Le Gallo, 92648 Boulogne Cedex, (FR), (Proprietor designated states: all)

INVENTOR:

ESKICIOGLU, Ahmet, Mursuit, Apartment 125, 8235 Lakeshore Trail, Indianapolis, IN 46250, (US)

BEYERS, William, Wesley, Jr., 1075 Arrow Wood Drive, Carmel, IN 46033-9046, (US)

LEGAL REPRESENTATIVE:

Kohrs, Martin (88661), Thomson multimedia 46, quai A. Le Gallo, 92648 Boulogne-Billancourt Cedex, (FR)

PATENT (CC, No, Kind, Date): EP 1110393 A1 010627 (Basic)
EP 1110393 B1 020529
WO 200013412 000309

APPLICATION (CC, No, Date): EP 99951394 990831; WO 99US19700 990831

PRIORITY (CC, No, Date): US 98501 P 980831

DESIGNATED STATES (Pub A): AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; (Pub B): DE; FR; GB; IT

INTERNATIONAL PATENT CLASS: H04N-005/913; H04N-007/167; H04N-007/24

NOTE:

No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200222	819
CLAIMS B	(German)	200222	754
CLAIMS B	(French)	200222	1016
SPEC B	(English)	200222	4458
Total word count - document A			0
Total word count - document B			7047
Total word count - documents A + B			7047

...SPECIFICATION program guide providers, and in certain cases internet service providers.

A system in accordance with the present invention may utilize **public key** technology. Typically, such a system utilizes one **public key** (corresponding to a smart card) for all service providers. Each smart card has stored therein a secret private key that can decrypt messages encrypted by the **public key** . The service provider sends a **conditional access** (**CA**) entitlement message (i.e., an Entitlement Control Message or ECM) in the bit stream encrypted by the **public key** that may contain the name of the service provider, and the name, time, and cost of the program. This message...

...services can be purchased by the user. At some appropriate preprogrammed time, the smart card causes the device (e.g., **set - top** box) to automatically place a telephone call to the **CA** center. Using a secure channel, the CA center in cooperation with a bank receives billing

information from the smart card...system, which may be utilized to manage access to copies of restricted programs, for example, scrambled (or encrypted) programs. A **conditional access** system may be integrated into a renewable security device, such as a smart card complying to the National Renewable Security Standard (NRSS), EIA-679 Part A or Part B. The **conditional access** system, when implemented within a digital television (DTV), **set - top** box (STB), or the like, permits a user to view only legitimate copies of the scrambled program. The functionality of the smart card may be embedded within the DTV or STB.

A **Certificate** Authority (not shown) issues digital **certificates** and **public** and private **key** pairs, which are used as explained below. It is within the scope of this invention that the role of the **certificate** authority may be performed by the service providers in collaboration with the manufacturers of the devices. A billing center may...the broadcasters, and the corresponding private key is placed in the tamper-proof NRSS-based smart cards, distributed by the **CA** providers to the consumers. This public key is used to protect the ECMs generated at the head-end. It is...

...than DES.

Symmetric key cryptography involves the use of the same key for both encryption and decryption. The foundation of **public - key** cryptography is the use of two related keys, one public and one private. The private key is a secret key, and it is computationally unfeasible to deduce the private key from the **public key** , which is publicly available. Anyone with a **public key** can encrypt a message, but only the person or device having the associated and predetermined private key can decrypt it.

A digital home network 10, as depicted in Figure 1, is a cluster of digital audio/visual (AN) devices including **set - top** -boxes 12, TVs 14, VCRs 16, DVD players 18 and general-purpose computing devices (not shown) such as personal computers...

9/3,K/6 (Item 6 from file: 348)

01116485

SECURITY MODEL FOR INTERACTIVE TELEVISION APPLICATIONS
SICHERHEITSMODEL FUR INTERAKTIVE FERNSEHANWENDUNG
MODELE DE SECURITE POUR APPLICATIONS DE TELEVISION INTERACTIVE

PATENT ASSIGNEE:
Open TV, INC., (2858191), 401 East Middlefield Road, Mountain View, CA 94043-4005, (US), (Proprietor designated states: all)
INVENTOR:
CHARI, Suresh, N., 343 West 87th Street, Apartment 5, New York, NY 10024, (US)
SZYMANSKI, Steven, 100 N. Whisman Road, Apartment 3215, Mountain View, CA 94043, (US)
MENAND, Jean-Rene, 1535 Siesta Drive, Los Altos, CA 94024, (US)
DUREAU, Vincent, 3519 South Court, Palo Alto, CA 94306, (US)
LEGAL REPRESENTATIVE:
Freeman, Jacqueline Carol (72181), W.P. THOMPSON & CO. Celcon House 289-293 High Holborn, London WC1V 7HU, (GB)

PATENT (CC, No, Kind, Date): EP 1080582 A1 010307 (Basic)
EP 1080582 B1 030319
WO 99063757 991209
APPLICATION (CC, No, Date): EP 99925831 990525; WO 99US11537 990525
PRIORITY (CC, No, Date): US 87386 980529; US 196964 981120
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04N-007/173; H04N-007/167
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count

CLAIMS B	(English)	200312	1530
CLAIMS B	(German)	200312	1687
CLAIMS B	(French)	200312	1757
SPEC B	(English)	200312	6991
Total word count - document A			0
Total word count - document B			11965
Total word count - documents A + B			11965

...SPECIFICATION accesses between carousels may also be employed for purposes of verifying the authenticity of carousels or modules received by a **set - top** box. A carousel (or more particularly its directory module) may contain a **certificate** encrypted with the private key of the producer. The **set - top** box, having a copy of the producer's **public key** , can verify that the carousel came from the producer by decrypting the **certificate** using the **public key** . The use of hash functions as described above may also be employed to ensure the authenticity of the non-directory...

9/3,K/7 (Item 7 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01114401

MODULE MANAGER FOR INTERACTIVE TELEVISION SYSTEM
MODULVERWALTER FUR INTERAKTIVES FERNSEHSYSTEM
GESTIONNAIRE DE MODULES POUR SYSTEME INTERACTIF DE TELEVISION

PATENT ASSIGNEE:
Open TV, INC., (2858191), 401 East Middlefield Road, Mountain View, CA 94043-4005, (US), (Proprietor designated states: all)

INVENTOR:
GOODMAN, Andrew, 2171 Avy Avenue, Menlo Park, CA 94025, (US)
MENAND, Jean, Rene, 1102 Embarcadero Road, Palo Alto, CA 94303, (US)

LEGAL REPRESENTATIVE:
Freeman, Jacqueline Carol (72181), W.P. THOMPSON & CO. Celcon House 289-293 High Holborn, London WC1V 7HU, (GB)

PATENT (CC, No, Kind, Date): EP 1082850 A1 010314 (Basic)
EP 1082850 B1 020417
WO 9962248 991202

APPLICATION (CC, No, Date): EP 99930127 990528; WO 99US11908 990528

PRIORITY (CC, No, Date): US 87269 980529

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04N-005/00; H04N-007/16

NOTE:
No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200216	1103
CLAIMS B	(German)	200216	1046
CLAIMS B	(French)	200216	1272
SPEC B	(English)	200216	5751
Total word count - document A			0
Total word count - document B			9172
Total word count - documents A + B			9172

...SPECIFICATION are stored in RAM 37, where they are available for use by applications executing in the control system 35. The **set** -top box may employ a security mechanism to ensure that the carousels and/or particular modules which are being downloaded...

...the private key. Likewise, a file which is encrypted with the private key can only be decrypted with the public **key** . Thus, when a **public - key** encrypted message is sent to the owner, the sender can be assured that, even if the message is intercepted, only...
...who holds the private key) can decrypt it and read the message.
The set-top box maintains copies of the **public keys** of one or more

CLAIMS B	(English)	200312	1530
CLAIMS B	(German)	200312	1687
CLAIMS B	(French)	200312	1757
SPEC B	(English)	200312	6991
Total word count - document A			0
Total word count - document B			11965
Total word count - documents A + B			11965

...SPECIFICATION accesses between carousels may also be employed for purposes of verifying the authenticity of carousels or modules received by a **set - top** box. A carousel (or more particularly its directory module) may contain a **certificate** encrypted with the private key of the producer. The **set - top** box, having a copy of the producer's **public key** , can verify that the carousel came from the producer by decrypting the **certificate** using the **public key** . The use of hash functions as described above may also be employed to ensure the authenticity of the non-directory...

9/3,K/7 (Item 7 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01114401

MODULE MANAGER FOR INTERACTIVE TELEVISION SYSTEM
MODULVERWALTER FUR INTERAKTIVES FERNSEHSYSTEM
GESTIONNAIRE DE MODULES POUR SYSTEME INTERACTIF DE TELEVISION

PATENT ASSIGNEE:
Open TV, INC., (2858191), 401 East Middlefield Road, Mountain View, CA 94043-4005, (US), (Proprietor designated states: all)

INVENTOR:
GOODMAN, Andrew, 2171 Avy Avenue, Menlo Park, CA 94025, (US)
MENAND, Jean, Rene, 1102 Embarcadero Road, Palo Alto, CA 94303, (US)

LEGAL REPRESENTATIVE:
Freeman, Jacqueline Carol (72181), W.P. THOMPSON & CO. Celcon House 289-293 High Holborn, London WC1V 7HU, (GB)

PATENT (CC, No, Kind, Date): EP 1082850 A1 010314 (Basic)
EP 1082850 B1 020417
WO 9962248 991202

APPLICATION (CC, No, Date): EP 99930127 990528; WO 99US11908 990528

PRIORITY (CC, No, Date): US 87269 980529

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04N-005/00; H04N-007/16

NOTE:
No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200216	1103
CLAIMS B	(German)	200216	1046
CLAIMS B	(French)	200216	1272
SPEC B	(English)	200216	5751
Total word count - document A			0
Total word count - document B			9172
Total word count - documents A + B			9172

...SPECIFICATION are stored in RAM 37, where they are available for use by applications executing in the control system 35. The **set** -top box may employ a security mechanism to ensure that the carousels and/or particular modules which are being downloaded...

...the private key. Likewise, a file which is encrypted with the private key can only be decrypted with the public **key** . Thus, when a **public** - **key** encrypted message is sent to the owner, the sender can be assured that, even if the message is intercepted, only...
...who holds the private key) can decrypt it and read the message.
The set-top box maintains copies of the **public keys** of one or more

trusted parties. When the set- **top** box receives a directory module, it checks the module for a certificate signed with the private key of the producer. The certificate contains a producer's certificate, which is the producer's **public key** , signed by a trusted party. The **set - top** box, having a copy of the trusted party's **public key** , can verify that the producer's certificate (the producer's **public key**) is authentic. Then, the producer's authenticated **public** key can be used to verify that the **certificate** is unaltered. The security mechanism may also include performing a hash function over the modules and including the hash value...

9/3,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01062087
CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS
SYSTEM MIT BEDINGTEM ZUGANG FUR DIGITALE EMPFANGER
SYSTEME D'ACCES CONDITIONNEL POUR RECEPTEURS NUMERIQUES
PATENT ASSIGNEE:
Thomson Licensing S.A., (2880640), 46, quai Alphonse Le Gallo, 92648 Boulogne Cedex, (FR), (Proprietor designated states: all)
INVENTOR:
ESKICIOGLU, Ahmet, Mursit, 8235 Lakeshore Trail 125, Indianapolis, IN 46250, (US)
OZKAN, Mehmet, Kemal, Savasci Sokak Bozokatt 19/1, Avcilar, 34840 Istanbul, (TR)
BEYERS, Billy, Wesley, Jr., 6920 Woodcrest Drive, Greenfield, IN 46104, (US)
LEGAL REPRESENTATIVE:
Kohrs, Martin et al (88662), Thomson multimedia 46, quai A. Le Gallo, 92100 Boulogne-Billancourt, (FR)
PATENT (CC, No, Kind, Date): EP 1040661 A1 001004 (Basic)
EP 1040661 B1 011031
WO 9930498 990617
APPLICATION (CC, No, Date): EP 98962970 981209; WO 98US26069 981209
PRIORITY (CC, No, Date): US 69063 P 971210
DESIGNATED STATES: DE; FR; GB; IE; IT
INTERNATIONAL PATENT CLASS: H04N-007/16
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200144	358
CLAIMS B	(German)	200144	364
CLAIMS B	(French)	200144	435
SPEC B	(English)	200144	1826
Total word count - document A			0
Total word count - document B			2983
Total word count - documents A + B			2983

...SPECIFICATION 0 658 054 discloses generating a descrambling key using two pieces of transmitted data.

Summary of the Invention
In a **conditional access** (**CA**) system, the signals are usually scrambled using symmetric ciphers such as the Data Encryption Standard (DES). For security reasons, the...

...few seconds. The protection of the descrambling keys, which need to be sent with the signals, is often provided by **public - key** cryptography. **Public - key** cryptography introduces problems associated with the **public key** infrastructure and distribution of the keys. This invention resides, in part, in recognition of the described problem and, in part... DTV 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a **cable television** SP 52, a

satellite system SP 54, and an internet SP 56. **Conditional Access** Organization (**CA**) 75 is not directly connected to either the service providers or STB 40 but deals with key management and issues **public** and private **key** pairs which may be used, if necessary, as explained below.

The present invention employs the concept of secret sharing which eliminates the requirement for using **public key** cryptography to ensure secure transmission of the audio/visual (A/V) stream from a service provider. A variation of a...

9/3,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01043254
AUTHORIZATION OF SERVICES IN A CONDITIONAL ACCESS SYSTEM
AUTORISIERUNG VON DIENSTEN IN EINEM SYSTEM MIT BEDINGTEM ZUGRIFF
AUTORISATION DE SERVICES DANS UN SYSTEME D'ACCES CONDITIONNEL
PATENT ASSIGNEE:
Scientific-Atlanta, Inc., (353663), 5030 Sugarloaf Parkway, Lawrenceville, GA 30044, (US), (Proprietor designated states: all)
INVENTOR:
AKINS, Glendon, L., III, 2510 Windward Lane, N.E., Gainesville, GA 30501, (US)
BANKER, Robert, O., 1581 Chamblee Gap Road, Cumming, GA 30040, (US)
PINDER, Howard, G., 4317 Stilson Circle, Norcross, GA 30092, (US)
WASILEWSKI, Anthony, J., 10680 Wren Ridge Road, Alpharetta, GA 30022, (US)
LEGAL REPRESENTATIVE:
Kugele, Bernhard et al (51541), NOVAPAT INTERNATIONAL SA, 9, Rue du Valais, 1202 Geneve, (CH)
PATENT (CC, No, Kind, Date): EP 1000508 A1 000517 (Basic)
EP 1000508 B1 011031
WO 9907148 990211
APPLICATION (CC, No, Date): EP 98939870 980731; WO 98US16028 980731
PRIORITY (CC, No, Date): US 54575 P 970801; US 127352 980731
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04N-007/16; H04N-007/167
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200144	1109
CLAIMS B	(German)	200144	1078
CLAIMS B	(French)	200144	1191
SPEC B	(English)	200144	28732
Total word count - document A			0
Total word count - document B			32110
Total word count - documents A + B			32110

...SPECIFICATION to MUX 200 encapsulated in EMM 111.

MSK 208 and other parts of EMM 111 are preferably encrypted using a **public key** algorithm, such as the well-known RSA algorithm, with a **public key** associated with the specific **set - top** box 113 to which the EMM is addressed. The **public keys** of all **set - top** boxes 113 in a system 101 are stored in **Public Key** Data Base 207. The **public keys** in this data base are preferably **certified** by a **certificate** authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In... unit(underscore)message 1011 will be examined in more detail later.

EMM Structure Details: FIG. 11

FIG. 11 shows a **CA** message 805 which contains an EMM 1112. CA message 805 has a header 1003, a CA EMM message 1101, and information is particularly sensitive and is consequently encrypted by both the **public key** of DHCT 333, for privacy reasons, and the private key of the entitlement agent or the **conditional access** authority, to apply a

digital signature. Upon reception, and after the privacy decryption, if the signature verification fails, the EMM is discarded by DHCT 333. Included in this information are an ID for the **conditional access** system, the type of the CA message, the serial number of the microprocessor in the DHCT's DHCTSE 627, an identifier for the CAA or EA which is the source of the EMM, an indication of which of the three **public keys** for the CAA in DHCT 333's secure element is to be used to decrypt the sealed digest, and an...

...of the operations performed using EMMs.
Details of DHCTSE 627: FIGs. 12-14
DHCTSE 627 has five main functions in **conditional access** system 601:
* It securely stores keys including the **public** and private **keys** for DHCT 333, **public keys** for the CAA, **public keys** for EAs from which DHCT 333 is authorized to receive services, and MSKs provided by those EAs.
* It securely stores...

...operations performed by DHCTSE 627, code for interpreting EMMs 1313, code for interpreting ECMs 1321, and code for handling other **CA** messages such as the FPM and the GBAM. Code 1307 includes code 1308 for the MD5 one-way hash algorithm, the code 1309 for the RSA **public key** algorithm, and the code 1311 for the 3DES algorithm. EMM code 1313 falls into three classes: code 1315 which interprets EMMs received from a **conditional access** authority, code 1317 which interprets EMMs employed by the entitlement agents to configure the storage allocation they receive from the...installed in DHCTSE 627 when DHCTSE 627 is manufactured.
In a preferred embodiment, the manufacturer of DHCT 333 maintains a **certified** database which has the serial number of each DHCT together with the pair of public keys belonging to it. When...
...keys for the DHCT. The manufacturer thus functions as the certification authority for the keys. Control suite 607 stores the **public keys** in a database of its own. For details on key certification, see Schneier, supra, pages 425-428. Getting the **public keys** for the DHCT from the manufacturer has two advantages: first, it solves the problem of certifying the keys; second, because the **public keys** come from the manufacturer and not from DHCT 333, there is no requirement in **conditional access** system 601 that DHCT 333 have a reverse path to control suite 607.
CAA keys 1329 are **public keys** for the **conditional access** authority. In a preferred embodiment, CAA keys 1329 include three **public keys** for the **conditional access** authority. These keys are originally installed when DHCTSE 627 is manufactured, but may be changed in response to EMMs, as...operator may have a plurality of EAs. In a preferred embodiment, there is a different EA and an associated EA **certificate** 2803 for every operating site of any given operator. This ensures that DHCTs can not be migrated between operational sites without the knowledge and participation of the operator CAAsignature 2802.
The geo-political **CA certificate** 2807 shown in FIG. 28, is not required to operate the normal **conditional access** and electronic activities of the operator. However, the operator may desire to link its signature chain into a larger chain...
...of the operator's DBDS. In this case, the signature chains may be readily linked to those of geo-political **CA** and its signature 2807 by having the **public keys** of one or all of the DHCT root signature 2804, the Root CAA signature 2808 or operator CAA signatures 2802 **certified** by the geo-political **CA** signature. This is accomplished by having a **certificate** placed in a database for each of the public keys associated with signatures 2804, 2808 and 2802. Said certificate is...

9/3,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01039291

SOURCE AUTHENTICATION OF DOWNLOAD INFORMATION IN A CONDITIONAL ACCESS SYSTEM

QUELLENAUTHENTIFIZIERUNG VON DATENFERNLADUNGSINFORMATION IN EINEM SYSTEM MIT BEDINGTEM ZUGANG

AUTHENTIFICATION DE LA SOURCE D'INFORMATIONS TELECHARGEES DANS UN SYSTEME D'ACCES CONDITIONNEL

PATENT ASSIGNEE:
Scientific-Atlanta, Inc., (353663), 5030 Sugarloaf Parkway, Lawrenceville, GA 30044, (US), (Proprietor designated states: all)
INVENTOR:
AKINS, Glendon, L., III, 2510 Windward Lane N.E., Gainesville, GA 30501, (US)
BANKER, Robert, O., 1581 Chamblee Gap Road, Cumming, GA 30040, (US)
PALGON, Michael, S., 1196 Poplar Grove Drive, Atlanta, GA 30306, (US)
PINDER, Howard, G., 4317 Stilson Circle, Norcross, GA 30092, (US)
WASILEWSKI, Anthony, J., 10680 Wren Ridge Road, Alpharetta, GA 30022, (US)
LEGAL REPRESENTATIVE:
Kugele, Bernhard et al (51541), Novagraaf SA 25, Avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)
PATENT (CC, No, Kind, Date): EP 1013091 A1 000628 (Basic)
EP 1013091 B1 020918
WO 99007149 990211
APPLICATION (CC, No, Date): EP 98939155 980731; WO 98US16040 980731
PRIORITY (CC, No, Date): US 54575 P 970801; US 127152 980731
DESIGNATED STATES: DE; FR; GB; IT; NL
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1189439 (EP 2001126558)
INTERNATIONAL PATENT CLASS: H04N-007/16; H04N-007/167
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200238	1352
CLAIMS B	(German)	200238	1301
CLAIMS B	(French)	200238	1636
SPEC B	(English)	200238	28358
Total word count - document A			0
Total word count - document B			32647
Total word count - documents A + B			32647

...SPECIFICATION to MUX 200 encapsulated in EMM 111.

MSK 208 and other parts of EMM 111 are preferably encrypted using a **public key** algorithm, such as the well-known RSA algorithm, with a **public key** associated with the specific **set - top** box 113 to which the EMM is addressed. The **public keys** of all **set - top** boxes 113 in a system 101 are stored in **Public Key** Data Base 207. The **public keys** in this data base are preferably **certified** by a **certificate** authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In... underscore)message 1011 will be examined in more detail later.

EMM Structure Details: FIG. 11

FIG. 11 shows a CA **message** 805 which contains an EMM 1112. CA message 805 has a header 1003, a CA EMM message 1101, and a...

...from the EMM(underscore)inside(underscore)header. This information is particularly sensitive and is consequently encrypted by both the public **key of** DHCT 333, for privacy reasons, and the private key of the entitlement agent or the conditional **access authority** , to apply a digital signature. Upon reception, and after the privacy decryption, if the signature verification fails, the EMM is discarded by DHCT 333. Included in this information are an ID for the conditional **access system** , the type of the CA message, the serial number of the microprocessor in the DHCT's DHCTSE 627, an identifier for the CAA or EA which is the source of the EMM, an indication of which of the three public **keys for** the CAA in DHCT 333's secure element is to be used to decrypt the sealed digest, and an indication...

9/3,K/40 **(Item 20 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT

00475793 **Image available**
VERIFICATION OF THE SOURCE OF PROGRAM OF INFORMATION IN A CONDITIONAL ACCESS SYSTEM
VERIFICATION DE LA SOURCE D'INFORMATION DE PROGRAMME DANS UN SYSTEME A ACCES CONDITIONNEL
Patent Applicant/Assignee:
SCIENTIFIC-ATLANTA INC,
Inventor(s):
AKINS Glendon L III,
BANKER Robert O,
PALGON Michael S,
PINDER Howard G,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9907145 A1 **19990211**
Application: WO 98US15753 19980731 (PCT/WO US9815753)
Priority Application: US 9754575 19970801; US 98126795 19980731
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 30356

Patent and Priority Information (Country, Number, Date):
Patent: ... **19990211**
Fulltext Availability:
Detailed Description
Publication Year: **1999**

Detailed Description
... the encryption system of the present invention uses symmetrical key encryption technique5 to encrypt and decrypt the service instance and **public** key encryption techniques to transport a copy of one of the keys used in the symmetrical key techniques of the...resulting encrypted streams are sent to MUX 200 to be combined with other elementary streams and private data, such as **conditional access** data. The key used in the Program Encrypt function 201 is called the Control Word (CW) 202. The CW 202...
...I I 1.

I 0
MSK 208 and other parts of EMM I I I are preferably encrypted using a **public key** algorithm, such as the well-known RSA algorithm, with a **public key** associated with the specific **set - top** box II 3 to which the EMM is addressed. The **public keys** of all **set - top** boxes I 1 3 in a system I 0 1 are stored in **Public Key** Data Base 207. The **public** keys in this data base are preferably certified by a **certificate** authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In...even-parity control will be examined in more detail later.

ENINI Structure Details: FIG. 11
FIG. I I shows a **CA** message 805 which contains an EMM 11 12. CA message 805 has a header 1003, a CA EMM message I...

...is inforn-iation from the EMM-inside-header. This information is particularly sensitive and is consequently encrypted by both the **public key** of DHCT 333, for privacy reasons, and the private key of the entitlement agent or the **conditional access** authority, to

of one or all of the DHCT root signature 2804, the Root CAA signature 2808 or operator CAA signatures 2802 **certified** by the geo-political **CA** signature. This is accomplished by having a **certificate** placed in a 76
database for each of the public keys associated with signatures 2804, 2808 and 2802.

Said certificate...

9/3,K/41 (Item 21 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00475750 **Image available**
REAL TIME BANK-CENTRIC UNIVERSAL PAYMENT SYSTEM
SYSTEME DE PAIEMENT UNIVERSEL DE CENTRALISATION BANCAIRE EN TEMPS REEL
Patent Applicant/Assignee:
HUNTINGTON BANCSHARES INCORPORATED,
HEWLETT-PACKARD COMPANY,
VERIFONE INC,
RANDLE William,
ERCOLE Richard,
GEER Terry L,
JAMES David L,
FREDELAKE Jodie M,
ROMAN Dennis,
FONTANA Fabio,
BARTLETT Rick,
ROSENBERG Ruth,
MURPHY Robert W,
TRAN Tuong T,
LAMPRU Paul,
Inventor(s):
RANDLE William,
ERCOLE Richard,
GEER Terry L,
JAMES David L,
FREDELAKE Jodie M,
ROMAN Dennis,
FONTANA Fabio,
BARTLETT Rick,
ROSENBERG Ruth,
MURPHY Robert W,
TRAN Tuong T,
LAMPRU Paul,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9907102 A1 **19990211**
Application: WO 98US15780 19980730 (PCT/WO US9815780)
Priority Application: US 97903102 19970730
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CA MX US
Publication Language: English
Fulltext Word Count: 8345
Patent and Priority Information (Country, Number, Date):
Patent: ... **19990211**
Fulltext Availability:
Detailed Description
Publication Year: **1999**

Detailed Description
... for certificates, the ECTS is a central certificate authority performing public key generation, the issuance and renewal of keys and **certificates** , and the manager of the **certificate** repository.

Linked with **public** **key** technology is the need for chip cards or smart

cards to securely store a private key to allow it to...

...but prevent its duplication. A goal for the ECTS is to foster the development of a national and international open **public key certification** infrastructure based on smart card technology. Finally, as in the traditional payments world, there is a requirement to **certify** hardware and software devices which interface with financial networks. Given the many access options, such as browsers, PC software, kiosks, ATM's, telephones and terminals, TV **set - tops** , personal digital assistants, etc., the ECTS will set standards and operate a streamlined and cost-effective **certification** process. The ECTS will provide value added services to its members and their customers within a privacy framework and will...

9/3,K/42 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00465715 **Image available**
GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES
ACCES CONDITIONNEL GLOBAL A DES SERVICES DE TELEDIFFUSION
Patent Applicant/Assignee:
THOMSON CONSUMER ELECTRONICS INC,
ESKICIOGLU Ahmet Mursit,
Inventor(s):
ESKICIOGLU Ahmet Mursit,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9856180 A1 **19981210**
Application: WO 98US11634 19980605 (PCT/WO US9811634)
Priority Application: US 9748852 19970606
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 4389

Patent and Priority Information (Country, Number, Date):
Patent: ... **19981210**
Fulltext Availability:
Detailed Description
Claims
Publication Year: **1998**

Detailed Description
... of the smart card may be considered to be a
SUBSTITUTE SHEET (RULE 26)
part of the functionality of the **set - top** box thus removing the "boundaries" created by the physical card body of the smart card.

STB 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a **cable television** SP 52, a satellite system SP 54, an internet SP 56, and an electronic event guide SP 58. **Certificate** authority (**CA**) 75 is not directly connected to either the service providers or STB 40 but issues digital **certificates** and **public** and private **key** pairs which are
used as explained below. A **set - top** box **public key** is provided to the
manufacturers of the devices and is stored therein before the product is shipped to the consumer. It is within the scope of this invention that the role of **certificate** authority 75 may be performed by the

16 The combination of Claim 15 wherein the device is a **set - top** box.

17 The combination of Claim 15 wherein the device is a digital television.
18 In combination in a system...

...card coupled thereto,
said device performing the steps of:
(a) receiving an electronic program guide, said guide having a digital **certificate** and a separate message corresponding to each event in said guide, each of said digital **certificates** being encrypted using a
first private key of said guide, said separate message being encrypted using a **public key** of the smart card and having an associated digital signature created using a second private key of said guide;
(b...

9/3,K/43 (Item 23 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00465714 **Image available**
CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES
SYSTEME D'ACCES CONDITIONNEL POUR BOITIERS DE RACCORDEMENT
Patent Applicant/Assignee:
THOMSON CONSUMER ELECTRONICS INC,
ESKICIOGLU Ahmet Mursit,
WEHMEYER Keith Reynolds,
VIRAG David Emery,
Inventor(s):
ESKICIOGLU Ahmet Mursit,
WEHMEYER Keith Reynolds,
VIRAG David Emery,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9856179 A1 **19981210**
Application: WO 98US11633 19980605 (PCT/WO US9811633)
Priority Application: US 9748819 19970606
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 4015

Patent and Priority Information (Country, Number, Date):
Patent: ... **19981210**
Fulltext Availability:
Detailed Description
Claims
Publication Year: **1998**

Detailed Description
... invention,
the first message comprises data associated with the first device and a date and time stamp, and the digital **certificate** comprises data associated with the second device and a second public key.

In accordance with another aspect of the present invention, the step of authenticating comprises decrypting the digital **certificate** using a first public key; decrypting the first encrypted

...e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital **certificate** received from said second device, said first **public key** being stored in
said first device;
(f) decrypting said first encrypted identification data using said second **public key** to generate a first decrypted identification data;
(g) authenticating said second device by comparing said first decrypted identification data to...

...second device second encrypted
identification data, said second encrypted identification data being encrypted in said first device using said second **public key** of said second device; and
(i) establishing a communication channel between said first and said second devices.
I 1. In combination in a system for managing access between a service provider and a **set - top** box having a smart card coupled thereto, said **set - top** box performing the steps of:
(a) sending a first message to the smart card, said first message containing **set - top** box identification data;
(b) receiving from the smart card, in response to said first message, a first digital **certificate** encrypted using a first private key, said first digital **certificate** containing service provider identificati6n
data;
(c) authenticating the smart card in response to said first digital certificate;
(d) contacting the...

...said second message
encrypted using a third private key;
(g) authenticating the service provider in response to said second digital **certificate** and said second encrypted message;
(h) providing confirmation of the authentication to the service provider; and
(i) establishing a communication...
...4. The combination of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second **public key** of said service provider.

15 The combination of Claim 14 wherein the step of authenticating the service provider comprises the steps of:
(a) decrypting said second digital certificate in the **set - top** box using said second **public key** ;
(b) decrypting said encrypted second message using a third **public key** to generate a second decrypted message; and
(c) comparing said second decrypted message to said second message.

16 The combination of Claim 15 wherein said first **public key** , said second **public key** , said first message and said second message are stored in said **set - top** box.

17 The combination of Claim 16 wherein said first digital certificate, said first private key and said first **public** key are issued
by an ...is stored in said smart card. with said service provider.
20 The combination of Claim 19 wherein said second digital **certificate** is stored in said service provider.

9/3,K/44 (Item 24 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00389791 **Image available**

RECEPTION APPARATUS FOR AUTHENTICATED ACCESS TO CODED BROADCAST SIGNALS
RECEPTEUR SERVANT A AUTHENTIFIER L'ACCES A DES SIGNAUX DE RADIODIFFUSION CODES

Patent Applicant/Assignee:
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY,
SAGER John Christopher,
Inventor(s):
SAGER John Christopher,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9730534 A1 **19970821**
Application: WO 97GB431 19970214 (PCT/WO GB9700431)
Priority Application: GB 963263 19960216
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
JP US AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 3902

Patent and Priority Information (Country, Number, Date):
Patent: ... **19970821**
Fulltext Availability:
Detailed Description
Publication Year: **1997**

Detailed Description
... Digital Video Broadcasting (DVB) applications) may be provided.

Whilst the receiver contains the necessary programs and a subsidiser association master **public key** Pbkm (assumed, for economy of receiver manufacture, to be common to all subsidisers), no information is contained in the read...

...receiver he will also purchase a 1 5 service package from the subsidiser, for which he will be supplied a **conditional access** module. The customer connects up the receiver and plugs in the **CA** module. The following process now takes place.

The first step 100 is an initialisation process which is a cryptographically authenticated...

9/3,K/45 (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00305317 **Image available**
APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM
APPAREIL ET PROCEDE POUR ETABLIR UNE LIAISON CRYPTOGRAPHIQUE ENTRE LES ELEMENTS D'UN SYSTEME
Patent Applicant/Assignee:
MERDAN GROUP INC,
Inventor(s):
ARNOLD Terry Sutton,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9523468 A1 **19950831**
Application: WO 95US2324 19950224 (PCT/WO US9502324)
Priority Application: US 94201399 19940224
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 29239

Patent and Priority Information (Country, Number, Date):

Patent: ... **19950831**
Fulltext Availability:
Detailed Description
Publication Year: **1995**

Detailed Description
... 100, the MKS-RS 102, the MKS-PS 104 and every PS 106 in the system will have its own **public** /private signature key pair. In addition, every ECS 108, every ECS-RS 1 1 0, ...other secure chips 140. The last or lowest level certificate will be a SC authentication certificate for the cable decoder **box** 116. This certificate will indicate that the PS 106 recognized the public signature key of the **cable decoder box** 1 1 6, and that the **cable decoder box** 1 1 6 is authorized to operate as a **cable decoder box** 1 1 6.

Thus, the PS 106 is the authority with respect to this second certificate, while the **cable decoder box** 1,16 is the subject. The combination of these two authentication certificates provides indirect authentication of the **cable decoder box** 116 by the MKS 100.

```
File   8:Ei Compendex(R) 1970-2004/Sep W2
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Aug
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Sep 09
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Sep W3
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Sep W2
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Aug W4
         (c)2004 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2004/Sep W3
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/Sep W2
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Sep W3
         (c) 2004 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Aug
         (c) 2004 The HW Wilson Co.
File 266:FEDRIP 2004/Jun
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2004/Jun W1
         (c) 2004 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2004/Aug
         (c) 2004 The HW Wilson Co
File 248:PIRA 1975-2004/Sep W2
         (c) 2004 Pira International
File  62:SPIN(R) 1975-2004/Jul W4
         (c) 2004 American Institute of Physics
File 239:Mathsci 1940-2004/Nov
         (c) 2004 American Mathematical Society

Set     Items   Description
S1       5254   SETTOP? ? OR SET()TOP? ? OR CONDITIONAL()ACCESS OR CABLE(1-
             W)(DEVICE? ? OR UNIT? ? OR APPARATUS?? OR MODULE? ? OR EQUIPM-
             ENT OR HARDWARE OR MACHINE OR BOX OR BOXES OR DECODER? ? OR R-
             ECEIVER? ? OR TRANSCEIVER? ? OR TERMINAL? ?)
S2      21290   (DIGITAL OR SATELLITE)()(TV OR TELEVISION)()RECEIVER? ? OR
             CABLE()(TV OR TELEVISION) OR CATV
S3      16551   PUBLIC(2W)KEY? ?
S4     707409   CA OR CENTRAL?(1W)(AGENT? ? OR AUTHORIT??? OR AUTHORIZ? OR
             AUTHORIS?) OR CERTIF?
S5         11   S1:S2 AND S3 AND S4
S6          7   RD (unique items)
S7     266845   KEY???(1W)(DATA OR INFORMATION OR VALUE? ? OR NUMBER? ? OR
             PARAMETER? ? OR VARIABLE? ?) OR SEED OR RANDOM?()(NUMBER? ? OR
              NUMERAL? ? OR BIT? ? OR BYTE? ? OR DATA OR INFORMATION)
S8       1290   S4(10N)S7
S9         28   S3 AND S8
S10        18   RD (unique items)
S11        13   S10 NOT (S6 OR PY=2000:2004)
S12        79   S1:S2(7N)MANUFACTURER? ?
S13         2   S3:S4 AND S12
```

6/5/1 **(Item 1 from file: 8)**
DIALOG(R)File 8:Ei Compendex(R)

06381399 E.I. No: EIP03207467857
Title: CA **-PK:** Conditional access **for broadcast networks**
Author: Nidd, M.; Husemann, D.
Corporate Source: IBM Research Zurich Research Laboratory, 8803 Ruschlikon, Switzerland
Source: Software - Practice and Experience v 33 n 5 Apr 25 2003. p 481-496
Publication Year: 2003
CODEN: SPEXBL ISSN: 0038-0644
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications)
Journal Announcement: 0305W3
Abstract: This paper presents a **conditional access** solution suitable for broadcast networks (e.g. Eureka-147 DAB, XM Radio's SDARS, etc.). This solution, called **CA** -PK (**Conditional Access** through **Public Keys**), can only be implemented in software, although it can utilize external crypto processors and allows a content provider to operate a **conditional access** system independently of third parties (i.e. DAB or GSM network operators). Furthermore, it integrates the consumer into the protection chain, creating a social environment that discourages illegal redistribution of access keys. 13 Refs.
Descriptors: Broadcasting; **Public key** cryptography; Computer software ; Bandwidth; Global system for mobile communications
Identifiers: Broadcast networks; **Conditional access**
Classification Codes:
716.1 (Information & Communication Theory); 723.2 (Data Processing)
716 (Electronic Equipment, Radar, Radio & Television); 723 (Computer Software, Data Handling & Applications)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA PROCESSING)

6/5/2 **(Item 1 from file: 65)**
DIALOG(R)File 65:Inside Conferences

04353476 INSIDE CONFERENCE ITEM ID: CN045602370
Public Key **Infrastructure: Using X.509** Certificates **For Device Authentication: Here A Cert, There A Cert, Everywhere A Cert**
Jones, D.
CONFERENCE: National Cable Television Association; Cable 2002-Annual convention; 51st
CABLE -CONVENTION-NATIONAL CABLE TELEVISION ASSOCIATION, 2002; 51ST P: 240-246
NCTA, 2002
ISBN: 0940272326
LANGUAGE: English DOCUMENT TYPE: Conference Technical papers
CONFERENCE EDITOR(S): Bell, M.; Greenfield, C.; Scott, A.
CONFERENCE SPONSOR: National Cable Television Association
CONFERENCE LOCATION: New Orleans, LA 2002; May (200205) (200205)

BRITISH LIBRARY ITEM LOCATION: 2943.950200
DESCRIPTORS: NCTA; **cable television** ; cable

6/5/3 **(Item 1 from file: 2)**
DIALOG(R)File 2:INSPEC

7977363 INSPEC Abstract Number: C2004-07-6130S-011
Title: Contract based late security binding
Author(s): Sakarelis, I.; Strang, T.; Dorsch, T.; Robertson, P.
Author Affiliation: Inst. for Commun. & Navigation, German Aerosp. Center, Wessling, Germany

Conference Title: EURESCOM. Powerful Networks for Profitable Services. Conference Proceedings p.175-84
Publisher: VDE Verlag GmbH, Berlin, Germany
Publication Date: 2002 Country of Publication: Germany 502 pp.
ISBN: 3 8007 2727 7 Material Identity Number: XX-2003-00930
Conference Title: EURESCOM Summit 2002
Conference Date: 21-24 Oct. 2002 Conference Location: Heidelberg, Germany
Medium: Also available on CD-ROM in PDF format
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: In this paper we describe a security architecture, that allows emerging computation platforms such as PDA's, **set - top** boxes and mobile phones to host a variety of applications in a secure fashion. We introduce a framework to distribute applications and associated security modules - so called security bodies - between the application developer, a trust center and the user's platform. We extend on currently known security frameworks and thereby introduce greater flexibility in the level of security and safety. Specifically, we define a security body associated with a signed application. This security body contains the **public key** for the application, as well as rules and software plug-ins governing the behaviour of the application at runtime. The active elements of the security body can take into account the current status at the end-user device, which may not be known in advance. We explore two procedures of interaction between a trust center and an application developer, the first one allowing a less restrictive **certification** procedure of applications. The second one gives the trust center direct control over signing each application release and also lets the trust center to validate applications in advance. A key feature is the fact, that application and security bodies, although they belong together, may be distributed separately. One application might even have several security bodies for different contexts. An important consequence for the end-user is that for each application he is provided with a trustworthy security configuration by default. (8 Refs)
Subfile: C
Descriptors: **certification** ; contracts; **public key** cryptography; software engineering
Identifiers: contract based late security binding; security architecture; security bodies; **public key** ; trust center; application developer; **certification** procedure; open software platform; legal contract
Class Codes: C6130S (Data security); C0230B (Legal aspects of computing); C0310F (Software development management)

6/5/4 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

7779973 INSPEC Abstract Number: B2003-12-6120D-043, C2003-12-6130S-053
Title: CA **-PK:** conditional access **for broadcast networks**
Author(s): Nidd, A.; Husemann, D.
Author Affiliation: Zurich Res. Lab., IBM Res., Ruschlikon, Switzerland
Journal: Software - Practice and Experience vol.33, no.5 p.481-96
Publisher: Wiley,
Publication Date: 25 April 2003 Country of Publication: UK
CODEN: SPEXBL ISSN: 0038-0644
SICI: 0038-0644(20030425)33:5L.481:CABN;1-H
Material Identity Number: S141-2003-005
U.S. Copyright Clearance Center Code: 0038-0644/03/$30.00
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: This paper presents a **conditional access** solution suitable for broadcast networks (e.g. Eureka-147 DAB, XM Radio's SDARS, etc.). This solution, called **CA** -PK (**Conditional Access** through **Public Keys**), can only be implemented in software, although it can utilize external crypto processors and allows a content provider to operate a **conditional access** system independently of third parties (i.e. DAB or GSM network operators). Furthermore, it integrates the consumer into the protection

chain, creating a social environment that discourages illegal redistribution of access keys. (13 Refs)
Subfile: B C
Descriptors: authorisation; digital radio; **public key** cryptography; telecommunication security
Identifiers: **CA** -PK; **conditional access** ; broadcast network access; Eureka-147 DAB; SDARS; **Conditional Access** through **Public Keys** ; digital radio; crypto processors; **conditional access** system; broadcast encryption; social environment; illegal key redistribution
Class Codes: B6120D (Cryptography); C6130S (Data security); C1260C (Cryptography theory)

6/5/5 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04336662 JICST ACCESSION NUMBER: 99A0708344 FILE SEGMENT: JICST-E
Information Security. Pay Mobile-Audio Broadcasting System.
AKIYAMA KOICHIRO (1); KAMIBAYASHI TOORU (1); YURA KOJI (1)
(1) Toshiba Corp.
Toshiba Rebyu(Toshiba Review), 1999, VOL.54,NO.7, PAGE.38-40, FIG.5, REF.1
JOURNAL NUMBER: F0360AAK ISSN NO: 0372-0462 CODEN: TORBA
UNIVERSAL DECIMAL CLASSIFICATION: 621.396+654.195 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: A pay broadcasting system is a **conditional - access** (**CA**) system which provides information only to those who have concluded the necessary contract. Current **CA** systems for satellite broadcasting offer high security by periodically transmitting **CA** information to each receiving apparatus. However, these systems are required to transmit a large amount of **CA** infromation. The need has therefore arisen for improvements to reduce the amount of **CA** information, especially in the case of mobile-audio broadcasting systems which have a restricted band and cannot expect to receive **CA** information regularly. In response to this problem, we have employed new concepts for both key configuration and event-driven transmission, which have decreased the amount of data to be transmitted. In addition, the application of advanced cryptographic technologies enable a system that is supported in the mobile environment to be as secure as current systems. (author abst.)
DESCRIPTORS: radio broadcast; message billing system; benefit principle; **public key** cryptography; cryptography key; digital signature; security system; dissemination of information; narrow band; digital method; contract; moving object; safety; current awareness; computer security
IDENTIFIERS: contents service; information security
BROADER DESCRIPTORS: broadcast; telecommunication; method; cryptogram; system; distribution of information; distribution(marketing); bandwidth ; object; property; information service; service; security; guarantee
CLASSIFICATION CODE(S): ND12020L; ND02030R

6/5/6 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

15496301 PASCAL No.: 02-0191708
A key transport protocol based on secret sharing: An application to conditional access **systems**
Security and watermarking of multimedia contents III : San Jose CA , **22-25 January 2001**
ESKICIOGLU Ahmet M
PING WAH WONG, ed
Thomson Multimedia, 101 West 103rd Street, INH 725, Indianapolis, IN

46290, United States
International Society for Optical Engineering, Bellingham WA, United States
Security and watermarking of multimedia contents. Conference, 3 (San Jose CA USA) 2001-01-22
Journal: SPIE proceedings series, 2001, 4314 139-148
ISBN: 0-8194-3992-4 ISSN: 1017-2653 Availability: INIST-21760; 354000097070770150
No. of Refs.: 14 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: United States
Language: English

In today's digital world, multimedia content is delivered to homes via the Internet, satellite, terrestrial and cable networks. Scrambling is a common approach used by **conditional access** systems to prevent unauthorized access to audio/visual data. The descrambling keys are securely distributed to the receivers in the same transmission channel. Their protection is an important part of the key management problem. Although **public - key** cryptography provides a viable solution, alternative methods are sought for economy and efficiency. This paper presents a key transport protocol based on secret sharing. It eliminates the need for a cipher, yet combines the advantages of symmetric and **public - key** ciphers.

English Descriptors: Alternative method; Transmission channel; Multimedia; Internet; **Public key** cryptography; Cable structure; Satellite; Secret sharing

French Descriptors: Methode alternative; Canal transmission; Multimedia; Internet; Cryptographie cle publique; Structure en cable; Satellite; Partage secret

Classification Codes: 001D04A04E; 001D04B03

6/5/7 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

14113145 PASCAL No.: 99-0308504
Fast encryption for set - top **technologies**
Multimedia computing and networking 1999 : San Jose CA , **25-27 January 1999**
LUCKS S; WEIS R; HILT V
KANDLUR Dilip D, ed; JEFFAY Kevin, ed; ROSCOE Timothy, ed
Theoretische Informatik, University of Mannheim, 68131 Mannheim, Germany; Praktische Informatik IV, University of Mannheim, 68131 Mannheim, Germany
International Society for Optical Engineering, Bellingham WA, United States.
Multimedia computing and networking. Conference (San Jose CA USA) 1999-01-25
Journal: SPIE proceedings series, 1998, 3654 84-94
ISBN: 0-8194-3125-7 ISSN: 1017-2653 Availability: INIST-21760; 354000084602560080
No. of Refs.: 47 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: United States
Language: English

In this paper we present two approaches to combine recent results of cryptographic research with the requirements of modern multimedia systems. The first is to evaluate modern block ciphers in a JAVA-environment. The second approach is based on recent developments regarding fast Luby-Rackoff ciphers. Paradoxically, it deals with doing "high-bandwidth encryption with low-bandwidth smartcards". SUP 6 Also, we discuss implementation considerations for a specific multimedia project, the multimedia database for teleteaching at the University of Mannheim.

English Descriptors: **Public key** cryptography; Object oriented programming; Information protection; Multimedia systems; Remote teaching; Computer security

French Descriptors: Cryptographie cle publique; Programmation orientee objet; Protection information; Systeme multimedia; Teleenseignement; Securite informatique

File 347:JAPIO Nov 1976-2004/May(Updated 040903)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200460
(c) 2004 Thomson Derwent

Set	Items	Description
S1	18591	SETTOP? ? OR SET()TOP? ? OR CONDITIONAL()ACCESS OR CABLE(1W)(DEVICE? ? OR UNIT? ? OR APPARATUS?? OR MODULE? ? OR EQUIPMENT OR HARDWARE OR MACHINE OR BOX OR BOXES OR DECODER? ? OR RECEIVER? ? OR TRANSCEIVER? ? OR TERMINAL? ?)
S2	14542	(DIGITAL OR SATELLITE)()(TV OR TELEVISION)()RECEIVER? ? OR CABLE()(TV OR TELEVISION) OR CATV
S3	3341	PUBLIC(2W)KEY? ?
S4	209278	AUTHORITY OR CA OR CERTIF?
S5	10	S1:S2 AND S3 AND S4
S6	42	S1:S2 AND S3
S7	32	S6 NOT S5
S8	23	S7 AND AC=US/PR
S9	14	S8 AND AY=(1970:1999)/PR
S10	10	S7 AND PY=1970:1999
S11	17	S9:S10
S12	209364	AUTHORITY OR CA OR CENTRAL(1W)AGENT? ? OR CERTIF? OR CENTRAL?(1W)(AUTHORIZ? OR AUTHORIS?)
S13	13	S1:S2 AND S3 AND S12
S14	0	S13 NOT S6
S15	795	S12(20N)S3
S16	255	S15 AND (TV OR TELEVISION OR VIDEO? OR CABLE? OR DIGITAL()VTR OR VOD OR NVOD OR PROGRAM? OR BROADCAST? OR SATELLITE)
S17	206843	CA OR CENTRAL?(1W)(AGENT? ? OR AUTHORIT??? OR AUTHORIZ? OR AUTHORIS?) OR CERTIF?
S18	244	S16 AND S17
S19	5	S18 AND (MANUFACTUR??? OR VENDOR? ? OR PRODUCER? ? OR DEVELOPER? ?)

5/5/1 **(Item 1 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

016358201 **Image available**

WPI Acc No: 2004-516105/200449

Related WPI Acc No: 2004-470098; 2004-479082; 2004-498500; 2004-505504; 2004-505597; 2004-505603; 2004-505605; 2004-505606; 2004-505632; 2004-505633; 2004-505634; 2004-505635; 2004-515843; 2004-515864; 2004-515908; 2004-515911; 2004-515914; 2004-515996; 2004-516042; 2004-516072; 2004-516077; 2004-516081; 2004-516128; 2004-516130; 2004-516131; 2004-516132; 2004-516133; 2004-516134; 2004-516135; 2004-516137; 2004-516138; 2004-516140; 2004-516143; 2004-516145; 2004-516146; 2004-516148; 2004-516149; 2004-516150; 2004-516151; 2004-516152; 2004-516153; 2004-516154; 2004-516155; 2004-516156; 2004-524472; 2004-551718; 2004-560891; 2004-569713; 2004-570227; 2004-591694; 2004-602961

XRPX Acc No: N04-408851

Information communication method in communication network, involves translating security code to Internet protocol address of one communication device, so that translated address remains anonymous to another communication device

Patent Assignee: BENNETT J (BENN-I); KARAOGUZ J (KARA-I)

Inventor: BENNETT J; KARAOGUZ J

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040117661	A1	20040617	US 2002432472	P	20021211	200449	B
			US 2003443894	P	20030130		
			US 2003457179	P	20030325		
			US 2003461717	P	20030410		
			US 2003465982	P	20030428		
			US 2003675774	A	20030930		

Priority Applications (No Type Date): US 2003675774 A 20030930; US 2002432472 P 20021211; US 2003443894 P 20030130; US 2003457179 P 20030325 ; US 2003461717 P 20030410; US 2003465982 P 20030428

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040117661	A1		26	H04L-009/00	Provisional application US 2002432472
					Provisional application US 2003443894
					Provisional application US 2003457179
					Provisional application US 2003461717
					Provisional application US 2003465982

Abstract (Basic): US 20040117661 A1

NOVELTY - A digital media containing security code such as pin code, is received from a communication device such as personal computer (PC). The security code is translated to Internet protocol (IP) address corresponding to another communication device such as media processing system (MPS), so that the translated address remains anonymous to PC. The media is routed to the MPS, based on the IP address.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) machine-readable storage medium storing computer program for communication of information; and

(2) system for communication of information in communication network.

USE - For communicating security information such as one-time **certificate** , device identification (ID), **public key** , code and device number between communication devices such as personal computer (PC) e.g. desktop PC, laptop computer, handheld computer, personal digital assistant (PDA) and other computing devices, media processing system (MPS) e.g. **set - top** box (STB), and television and media peripheral devices e.g. digital camera, digital camcorder, MP3 player, compact disk (CD) player, DVD player and windows media audio (WMA) player in communication network e.g. media exchange network.

ADVANTAGE - Facilitates secure communication of information between the communication devices, by maintaining the address of specific communication device as anonymous to another device.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart illustrating the process of providing secure anonymity using proxy server on media exchange network.

pp; 26 DwgNo 2A/11

Title Terms: INFORMATION; COMMUNICATE; METHOD; COMMUNICATE; NETWORK; TRANSLATION; SECURE; CODE; PROTOCOL; ADDRESS; ONE; COMMUNICATE; DEVICE; SO; TRANSLATION; ADDRESS; REMAINING; COMMUNICATE; DEVICE

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/00

File Segment: EPI

5/5/2 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

016320337 **Image available**

WPI Acc No: 2004-478232/200445

Related WPI Acc No: 1996-465320; 1997-363998; 1999-154174; 1999-154175; 1999-154176; 1999-154177; 1999-154178; 1999-154179; 1999-181268; 1999-243551; 2002-060946; 2002-499082; 2002-705909; 2002-722051; 2002-722052; 2003-677663; 2003-898213; 2004-155029; 2004-579235; 2004-623798

XRPX Acc No: N04-376950

Program provision method in conditional access **system e.g.** cable television **system, involves multiplexing encrypted digital bit streams, to provide partial encrypted stream**

Patent Assignee: PINDER H G (PIND-I); WASILEWSKI A J (WASI-I)

Inventor: PINDER H G; WASILEWSKI A J

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040107350	A1	20040603	US 95415617	A	19950403	200445	B
			US 957962	P	19951204		
			US 95580759	A	19951229		
			US 96767535	A	19961216		
			US 9754575	P	19970801		
			US 9754578	P	19970801		
			US 98111958	A	19980708		
			US 98126783	A	19980731		
			US 2000487076	A	20000119		
			US 2001930901	A	20010816		
			US 2003602988	A	20030625		

Priority Applications (No Type Date): US 2003602988 A 20030625; US 95415617 A 19950403; US 957962 P 19951204; US 95580759 A 19951229; US 96767535 A 19961216; US 9754575 P 19970801; US 9754578 P 19970801; US 98111958 A 19980708; US 98126783 A 19980731; US 2000487076 A 20000119; US 2001930901 A 20010816

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040107350	A1		57	H04K-001/00	CIP of application US 95415617 Provisional application US 957962 CIP of application US 95580759 CIP of application US 96767535 Provisional application US 9754575 Provisional application US 9754578 CIP of application US 98111958 Cont of application US 98126783 Cont of application US 2000487076 Cont of application US 2001930901 CIP of patent US 5742677 CIP of patent US 5870474 CIP of patent US 6005938 Cont of patent US 6292568

Abstract (Basic): US 20040107350 A1

NOVELTY - A selected digital bit stream comprising a packet identifier for identifying video, audio and data stream, is encrypted according to encryption process to provide the encrypted steams. The encrypted streams are multiplexed to provide partial encrypted stream.

USE - For providing program in **conditional access** system e.g. **cable television** (**CATV**) system for satellite television company or **cable television** (**CATV**) company.

ADVANTAGE - Minimizes piracy concerns in the **cable television** system.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram illustrating relationship between transaction encryption device and **conditional access** system.

key database (2411)

key **certification authority** (2413)

network (2415)

public key database (2421)

physically secure area (2428)

pp; 57 DwgNo 24/29

Title Terms: PROGRAM; PROVISION; METHOD; CONDITION; ACCESS; SYSTEM; CABLE; TELEVISION; SYSTEM; MULTIPLEX; ENCRYPTION; DIGITAL; BIT; STREAM; ENCRYPTION; STREAM

Derwent Class: T01; W01; W02

International Patent Class (Main): H04K-001/00

International Patent Class (Additional): H04L-009/00

File Segment: EPI

5/5/3 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

015081868 **Image available**

WPI Acc No: 2003-142386/200314

XRPX Acc No: N03-113082

Scalable content protection-enabled device e.g. audio/video receiver, authenticates destination device as strong/weakly protected device by verifying received certificate **with** certifying authority **/local** public key

Patent Assignee: KONINK PHILIPS ELECTRONICS NV (PHIG)

Inventor: BOUSIS L P F

Number of Countries: 101 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1271875	A1	20030102	EP 2001202382	A	20010621	200314	B
WO 200301764	A1	20030103	WO 2002IB2415	A	20020620	200314	
KR 2003027066	A	20030403	KR 2003702566	A	20030221	200353	
BR 200205665	A	20030729	BR 20025665	A	20020620	200365	
			WO 2002IB2415	A	20020620		
EP 1402701	A1	20040331	EP 2002735904	A	20020620	200424	
			WO 2002IB2415	A	20020620		
AU 2002309194	A1	20030108	AU 2002309194	A	20020620	200460	

Priority Applications (No Type Date): EP 2001202382 A 20010621

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1271875	A1	E	20	H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

WO 200301764 A1 E H04L-029/06

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

KR 2003027066 A H04L-009/32

BR 200205665 A H04L-029/06 Based on patent WO 200301764
EP 1402701 A1 E H04L-029/06 Based on patent WO 200301764
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR
AU 2002309194 A1 H04L-029/06 Based on patent WO 200301764

Abstract (Basic): EP 1271875 A1

NOVELTY - An authentication unit (114) of a source device (110) authenticates a destination device (130) as a strongly protected device, when a **certificate** for **public key** from the destination device is verified successfully with available **public key** of a **certifying authority** (CAPK). The destination device is authenticated as weakly protected device, when the **certificate** is verified successfully with locally available **public key** (SPK).

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Remote device authentication method; and

(2) Computer program product for authenticating remote device.

USE - Scalable content protection enabled device such as audio/video receivers and players, **set top** boxes, general purpose computers, mobile telephones, Internet applications.

ADVANTAGE - By authenticating the devices as weakly protected and strongly protected devices, the data is transmitted securely between the devices. Hence, data transfer efficiency is enhanced.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of the scalable content protection enabled device.

Source device (110)

Authentication unit (114)

Destination device (130)

pp; 20 DwgNo 1/8

Title Terms: CONTENT; PROTECT; ENABLE; DEVICE; AUDIO; VIDEO; RECEIVE; DESTINATION; DEVICE; STRONG; WEAK; PROTECT; DEVICE; VERIFICATION; RECEIVE ; **CERTIFY** ; **CERTIFY** ; AUTHORISE; LOCAL; PUBLIC; KEY

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/32; H04L-029/06

File Segment: EPI

5/5/4 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014919117 **Image available**

WPI Acc No: 2002-739824/200280

Related WPI Acc No: 2002-665867

XRPX Acc No: N02-582827

One-time password communication method for secure computer network access, involves activating random password after verification of digital certificate and digital signature received from client computer

Patent Assignee: ARCOT SYSTEMS INC (ARCO-N); JERDONEK R A (JERD-I)

Inventor: JERDONEK R; JERDONEK R A

Number of Countries: 101 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020095507	A1	20020718	US 2001262875	P	20010117	200280	B
			US 2001896560	A	20010628		
WO 200258357	A2	20020725	WO 2002US1673	A	20020117	200280	
NO 200303202	A	20030829	WO 2002US1673	A	20020117	200365	
			NO 20033202	A	20030715		
EP 1352502	A2	20031015	EP 2002709110	A	20020117	200368	
			WO 2002US1673	A	20020117		
AU 2002243613	A1	20020730	AU 2002243613	A	20020117	200427	

Priority Applications (No Type Date): US 2001262875 P 20010117; US 2001896560 A 20010628; US 2001896163 A 20010628

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020095507	A1		15	G06F-015/16	Provisional application US 2001262875

WO 200258357 A2 E H04L-029/00
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW
NO 200303202 A H04L-000/00
EP 1352502 A2 E H04L-029/06 Based on patent WO 200258357
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR
AU 2002243613 A1 H04L-029/00 Based on patent WO 200258357

Abstract (Basic): US 20020095507 A1

NOVELTY - A challenge comprising an inactive random password is provided to a client computer from an authentication server (350) through an external server (310). A digital **certificate** comprising an encrypted **public key** and a digital signature are obtained in response to the challenge from the client computer (300). The random password is activated by the authentication server after verification of the challenge response.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Password activation method in verification server; and

(2) One-time password utilization method.

USE - For obtaining and using one-time passwords for secure access to computer networks or systems that include a firewall, a VPN gateway from user appliances such as notebook computers, TV **set - top** boxes e.g. WEB TV game consoles e.g. PLAYSTATION, network computers, PDAs, WAP-enabled cellular devices, kiosks, computer-implemented wrist watches, wearable computers, kitchen appliances, surveillance equipment, pocket or portable displays or terminals, etc., for electronic mail servers, wireless application, secure distributed services access, embedded applications, financial transactions e.g. credit-card transaction system.

ADVANTAGE - Provides one-time passwords for secure access to computer networks, and eliminates need for authentication server or external server to preregister a hardware Key' or token'. Does not require precise synchronization between devices.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram explaining the pre-authentication process.

Client computer (300)

External server (310)

Authentication server (350)

pp; 15 DwgNo 3/5

Title Terms: ONE; TIME; PASSWORD; COMMUNICATE; METHOD; SECURE; COMPUTER; NETWORK; ACCESS; ACTIVATE; RANDOM; PASSWORD; AFTER; VERIFICATION; DIGITAL ; **CERTIFY** ; DIGITAL; SIGNATURE; RECEIVE; CLIENT; COMPUTER

Derwent Class: T01; W01

International Patent Class (Main): G06F-015/16; H04L-000/00; H04L-029/00; H04L-029/06

International Patent Class (Additional): G06F-001/00; H04L-009/00

File Segment: EPI

5/5/5 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014397968 **Image available**

WPI Acc No: 2002-218671/200228

XRPX Acc No: N02-167709

Transmitter for cable television **, stores information relating to latest** public key certificate **information and associated lapse information in leaf and container entries of directory**

Patent Assignee: SONY CORP (SONY); GONNO Y (GONN-I); NISHIO F (NISH-I); TSUNODA T (TSUN-I); YAMAGISHI Y (YAMA-I)

Inventor: GONNO Y; NISHIO F; TSUNODA T; YAMAGISHI Y
Number of Countries: 028 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1148676	A2	20011024	EP 2001303524	A	20010418	200228	B
JP 2001308841	A	20011102	JP 2000120940	A	20000421	200228	
US 20020059519	A1	20020516	US 2001839872	A	20010420	200237	

Priority Applications (No Type Date): JP 2000120940 A 20000421
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1148676	A2	E	53	H04L-009/32	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR				
JP 2001308841	A		34	H04L-009/08	
US 20020059519	A1			H04L-009/00	

Abstract (Basic): EP 1148676 A2

NOVELTY - A detector detects change of layer structure of directory, which stores **public key certificate** information. Based on detection result, differential information corresponding to change is obtained and transmitted to network. The information relating to latest **public key certificate** and associated lapse information is stored in container and leaf entries of directory.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Transmitting method;
(b) Receiver;
(c) Receiving method;
(d) Transmitting and receiving system;
(e) Transmitting and receiving method

USE - For **cable television** (**CATV**).

ADVANTAGE - Prevents wiretapping of information, manipulation or pretension using **public key** infrastructure and operates encryption communication with high efficiency. By processing the search request of lapsed information of **public key certification** , the directory servers efficiency is improved.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of encryption communication.

pp; 53 DwgNo 26/28

Title Terms: TRANSMIT; CABLE; TELEVISION; STORAGE; INFORMATION; RELATED; LATE; PUBLIC; KEY; **CERTIFY** ; INFORMATION; ASSOCIATE; LAPSE; INFORMATION; LEAF; CONTAINER; ENTER; DIRECTORY
Derwent Class: W01; W02
International Patent Class (Main): H04L-009/00; H04L-009/08; H04L-009/32
International Patent Class (Additional): G06F-012/00; G09C-001/00
File Segment: EPI

5/5/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013858827 **Image available**
WPI Acc No: 2001-343040/200136
XRPX Acc No: N01-248456

Electronic transaction method for on-line shopping, involves encrypting the purchase/service request from consumer and forwarding the request along with consumer public key **and** certificate

Patent Assignee: GEN INSTR CORP (GENN)
Inventor: SAFADI R
Number of Countries: 095 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200115092	A2	20010301	WO 2000US21232	A	20000803	200136	B
AU 200063988	A	20010319	AU 200063988	A	20000803	200136	
EP 1210694	A2	20020605	EP 2000950969	A	20000803	200238	
			WO 2000US21232	A	20000803		

KR 2002021413	A	20020320	KR 2002702356	A	20020223	200264
CN 1421024	A	20030528	CN 2000814406	A	20000803	200357
JP 2003526840	W	20030909	WO 2000US21232	A	20000803	200360
			JP 2001519377	A	20000803	
BR 200013513	A	20030819	BR 200013513	A	20000803	200367
			WO 2000US21232	A	20000803	

Priority Applications (No Type Date): US 99150679 P 19990825
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200115092	A2	E	49	G07F-000/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

AU 200063988	A		G07F-000/00	Based on patent WO 200115092
EP 1210694	A2	E	G07F-007/08	Based on patent WO 200115092

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

KR 2002021413	A		G06F-017/60	
CN 1421024	A		G07F-007/08	
JP 2003526840	W	34	G06F-017/60	Based on patent WO 200115092
BR 200013513	A		G06F-017/60	Based on patent WO 200115092

Abstract (Basic): WO 200115092 A2
NOVELTY - A specific goods/service request is selected by consumer terminal (145) using entertainment terminal (100). A purchase/service request is encrypted and sent to transaction server (150) along with consumer **public key** and **certificate** . Encrypted response including transaction information is provided from the server to consumer terminal. Response message is decrypted and the payment for purchase is arranged.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for electronic transaction system.
USE - For on-line shopping, electronic commerce.
ADVANTAGE - Provides effective transaction security even in the existing **cable television** networks, thereby promotes consumer service.
DESCRIPTION OF DRAWING(S) - The figure shows block diagram of e-commerce system on which electronic transaction method is applied.
Entertainment terminal (100)
Consumer terminal (145)
Transaction server (150)
pp; 49 DwgNo 2/2
Title Terms: ELECTRONIC; TRANSACTION; METHOD; LINE; SHOPPING; PURCHASE; SERVICE; REQUEST; CONSUME; FORWARDING; REQUEST; CONSUME; PUBLIC; KEY; **CERTIFY**
Derwent Class: W02
International Patent Class (Main): G06F-017/60; G07F-000/00; G07F-007/08
International Patent Class (Additional): H04N-007/173
File Segment: EPI

5/5/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013474942 **Image available**
WPI Acc No: 2000-646885/200062
Related WPI Acc No: 2000-506033; 2000-548857; 2000-647486; 2001-060711; 2001-070448
XRPX Acc No: N00-479409
Encrypted message authentication method in telecommunication systems uses secured transactions, involves determining whether received message is authentic and transferring decrypted message to host computer
Patent Assignee: GEN INSTR CORP (GENN)

Inventor: MORONEY P
Number of Countries: 091 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200045273	A1	20000803	WO 2000US2101	A	20000128	200062	B
AU 200035841	A	20000818	AU 200035841	A	20000128	200062	
EP 1163589	A1	20011219	EP 2000914452	A	20000128	200206	
			WO 2000US2101	A	20000128		
JP 2002540443	W	20021126	JP 2000596463	A	20000128	200307	
			WO 2000US2101	A	20000128		

Priority Applications (No Type Date): US 99128772 P 19990409; US 99117788 P 19990129
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200045273	A1	E	16	G06F-012/14	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW					
AU 200035841	A			G06F-012/14	Based on patent WO 200045273
EP 1163589	A1	E		G06F-012/14	Based on patent WO 200045273
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 2002540443	W		18	G09C-001/00	Based on patent WO 200045273

Abstract (Basic): WO 200045273 A1

NOVELTY - A secure processor (22) decrypts and authenticates the received encrypted message. Then, the secured processor determines whether the message is authentic and if so, the decrypted message is transferred to the host processor.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for method of providing secure processing in telecommunication system.

USE - For authenticating encrypted message using **public key** systems (PKS) also known as asymmetric system or crypto systems in telecommunication system requiring secured transactions such as cable telephony system, and banking application. Also in Internet, **cable television** , satellite.

ADVANTAGE - The message can be decrypted, at the same time the signature is verified. So the speed is improved due to such parallel processing. No need to protect the **certificates** in secure memory, since they are already cryptographically protected with a digital signature. Some of the encrypted information can still be decrypted and transferred to the host. This is useful for service or trouble shooting as where a key is expired and the secured processor gives notice of expiration date of key, **certificate** etc. Improves communication speed by using parallel processing.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart showing the basic steps of encrypted message authentication method.

pp; 16 DwgNo 1/2

Title Terms: ENCRYPTION; MESSAGE; AUTHENTICITY; METHOD; TELECOMMUNICATION; SYSTEM; SECURE; TRANSACTION; DETERMINE; RECEIVE; MESSAGE; AUTHENTICITY; TRANSFER; MESSAGE; HOST; COMPUTER
Derwent Class: P85; T01; W01
International Patent Class (Main): G06F-012/14; G09C-001/00
International Patent Class (Additional): G06F-015/00; H04L-009/32; H04M-001/67
File Segment: EPI; EngPI

5/5/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012933911 **Image available**
WPI Acc No: 2000-105758/200009

Related WPI Acc No: 1999-444261; 2000-106431
XRPX Acc No: N00-081236

Information leakage prevention device for smart cards and other cryptosystems

Patent Assignee: CRYPTOGRAPHY RES INC (CRYP-N); JAFFE J M (JAFF-I); JUN B C (JUNB-I); KOCHER P C (KOCH-I)
Inventor: JAFFE J M; JUN B C; KOCHER P C
Number of Countries: 084 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9963696	A1	19991209	WO 99US12565	A	19990603	200009 B
AU 9952038	A	19991220	AU 9952038	A	19990603	200021
EP 1084543	A1	20010321	EP 99937153	A	19990603	200117
			WO 99US12565	A	19990603	
US 6327661	B1	20011204	US 9887880	P	19980603	200203
			US 99326222	A	19990603	
US 20020124178	A1	20020905	US 9870344	P	19980102	200260
			US 9887826	P	19980603	
			US 9887880	P	19980603	
			US 9889529	P	19980615	
			US 98224682	A	19981231	
			US 99324798	A	19990603	
			US 99326222	A	19990603	
			US 2000737182	A	20001213	
			US 2001930836	A	20010815	
			US 20015105	A	20011203	

Priority Applications (No Type Date): US 9887880 P 19980603; US 99326222 A 19990603; US 9870344 P 19980102; US 9887826 P 19980603; US 9889529 P 19980615; US 98224682 A 19981231; US 99324798 A 19990603; US 2000737182 A 20001213; US 2001930836 A 20010815; US 20015105 A 20011203
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9963696	A1	E	34	H04K-001/00	
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 9952038	A			H04K-001/00	Based on patent WO 9963696
EP 1084543	A1	E		H04K-001/00	Based on patent WO 9963696
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
US 6327661	B1			G06F-012/14	Provisional application US 9887880
US 20020124178	A1			G06F-012/14	Provisional application US 9870344
					Provisional application US 9887826
					Provisional application US 9887880
					Provisional application US 9889529
					Div ex application US 98224682
					Cont of application US 99324798
					CIP of application US 99326222
					CIP of application US 2000737182
					CIP of application US 2001930836
					Cont of patent US 6278783
					Div ex patent US 6304658
					CIP of patent US 6327661
					CIP of patent US 6381699

Abstract (Basic): WO 9963696 A1

NOVELTY - A processor is connected to an interface (210) for cryptographically processing the quantity received by an input interface. The processor uses unpredictable information to conceal correlation between externally monitorable signals and secret during processing of the quantity.

DETAILED DESCRIPTION - An interface (210) receives the quantity to be cryptographically processed. An information source produces

unpredictable information. The interface (210) outputs the cryptographically processed quantity to a recipient. An INDEPENDENT CLAIM is also included for the method for preventing leakage of information from smart cards and other cryptosystems.

USE - For preventing information leakage from smart cards, cryptographic tokens, stored value cards and system, credit and debit cards, customer royalty cards, cryptographic accelerator, gambling and wagering system, cryptographic chips, tamper-resistant microprocessor, cryptographic PCMCIA cards for key management devices, banking pay management systems, secure web servers, electronic payment systems, micropayment systems and meters, prepaid telephone cards, identity verification systems, electronic funds transfer system, automatic teller machines, point of sale terminals, **certificate** issuance systems, electronic badges, door entry systems, physical locks using cryptographic keys, systems for decrypting television signals e.g. broadcast television, satellite television, **cable television** , systems for decrypting enciphered music, system for protecting video signals, copy protection systems, cellular telephone scrambling and authentication systems, key storage device for telephones and cryptographic data auditing systems.

ADVANTAGE - Protects information from external monitoring attacks by reducing signal to noise ratio of useful information leaked during processing. Prevents unauthorized copying or use of movies, audio content, computer programs, video games, images, text, databases etc.

DESCRIPTION OF DRAWING(S) - The figure illustrates the information leakage prevention apparatus.

Interfaces (210)

pp; 34 DwgNo 2/2

Title Terms: INFORMATION; LEAK; PREVENT; DEVICE; SMART; CARD
Derwent Class: T01; T04; W01
International Patent Class (Main): G06F-012/14; H04K-001/00
International Patent Class (Additional): G06F-011/30
File Segment: EPI

5/5/9 (Item 9 from file: 350)

012240108 **Image available**
WPI Acc No: 1999-046216/199904
XRPX Acc No: N99-033716

Conditional access **system for** set - top **box - uses** set - top **box to establish communication channel after authentication of service provider and smart card using** public **and private** key **pairs and digital** certificate

Patent Assignee: THOMSON CONSUMER ELECTRONICS INC (THOH); THOMSON CONSUMER ELECTRONICS SA (THOH)
Inventor: ESKICIOGLU A M; VIRAG D E; WEHMEYER K R
Number of Countries: 082 Number of Patents: 012
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9856179	A1	19981210	WO 98US11633	A	19980605	199904	B
AU 9877258	A	19981221	AU 9877258	A	19980605	199919	
EP 986910	A1	20000322	EP 98925263	A	19980605	200019	
			WO 98US11633	A	19980605		
BR 9809911	A	20000801	BR 989911	A	19980605	200043	
			WO 98US11633	A	19980605		
CN 1259260	A	20000705	CN 98805839	A	19980605	200052	
AU 732576	B	20010426	AU 9877258	A	19980605	200128	
MX 9911219	A1	20000601	MX 9911219	A	19991203	200133	
KR 2001013259	A	20010226	KR 99711251	A	19991201	200154	
JP 2002503354	W	20020129	WO 98US11633	A	19980605	200211	
			JP 99502920	A	19980605		
EP 986910	B1	20020814	EP 98925263	A	19980605	200255	
			WO 98US11633	A	19980605		
DE 69807221	E	20020919	DE 607221	A	19980605	200269	
			EP 98925263	A	19980605		

				WO 98US11633	A	19980605	
KR 374232	B	20030303	WO	98US11633	A	19980605	200349
			KR	99711251	A	19991201	

Priority Applications (No Type Date): US 9748819 P 19970606
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9856179	A1	E	26	H04N-007/167	
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW					
AU 9877258	A				Based on patent WO 9856179
EP 986910	A1	E		H04N-007/167	Based on patent WO 9856179
Designated States (Regional): DE FR GB IT					
BR 9809911	A			H04N-007/167	Based on patent WO 9856179
CN 1259260	A			H04N-007/167	
AU 732576	B			H04N-007/167	Previous Publ. patent AU 9877258
					Based on patent WO 9856179
MX 9911219	A1			H04N-007/167	
KR 2001013259	A			H04N-007/167	
JP 2002503354	W		29	G09C-001/00	Based on patent WO 9856179
EP 986910	B1	E		H04N-007/167	Based on patent WO 9856179
Designated States (Regional): DE FR GB IT					
DE 69807221	E			H04N-007/167	Based on patent EP 986910
					Based on patent WO 9856179
KR 374232	B			H04N-007/167	Previous Publ. patent KR 2001013259
					Based on patent WO 9856179

Abstract (Basic): WO 9856179 A

A smart card (30) is inserted into or coupled with a smart card reader in a **set - top** box (20) and data are exchanged through an internal bus (25). The smart card may be integrated into the box connected to a service provider (40) via a dial-up link or direct link (45) and a **certificate authority** (50) issues digital **certificates** and **public** and private **key** pairs. **Conditional access** is based on authentication of each device communicating with the **set - top** box before establishing a channel to the service provider.

This is carried out using a **public key** stored in the box, passing a message to the smart card containing identification data and verifying the smart card has returned a valid **certificate** , involving decrypting the first digital **certificate** using the **public key** . After authentication, the desired provider is contacted and confirmation of authentication is sent encrypted using the **public key** . The box establishes a channel with the provider and communication is then handled using **public - key** cryptology and the **public** and private **key** pairs associated with the service provider.

USE - Providing of **conditional access** to **set - top** box coupled to TV receiver

ADVANTAGE - Use of single **set - top** box with many service providers

Dwg.1/3

Title Terms: CONDITION; ACCESS; SYSTEM; SET; TOP; BOX; SET; TOP; BOX; ESTABLISH; COMMUNICATE; CHANNEL; AFTER; AUTHENTICITY; SERVICE; SMART; CARD; PUBLIC; PRIVATE; KEY; PAIR; DIGITAL; **CERTIFY**
Derwent Class: P85; W01; W02; W03
International Patent Class (Main): G09C-001/00; H04N-007/167
International Patent Class (Additional): H04L-009/32; H04N-005/00; H04N-007/16
File Segment: EPI; EngPI

5/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010355315 **Image available**
WPI Acc No: 1995-256629/199534
XRPX Acc No: N95-198094

Conditional programme access method e.g. for television - encrypting broadcast and checking user access status using messages with first part containing public key **and second part programme-specific encryption information**

Patent Assignee: FRANCE TELECOM (ETFR); TELEDIFFUSION DE FRANCE SA (TELG); TELEDIFFUSION DE FRANCE (TELG)
Inventor: COUTROT F
Number of Countries: 020 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2715256	A1	19950721	FR 94528	A	19940119	199534	B
WO 9520280	A1	19950727	WO 95FR55	A	19950118	199535	
EP 740870	A1	19961106	EP 95907046	A	19950118	199649	
			WO 95FR55	A	19950118		
US 5615265	A	19970325	US 94359597	A	19941220	199718	
EP 740870	B1	19981104	EP 95907046	A	19950118	199848	
			WO 95FR55	A	19950118		

Priority Applications (No Type Date): FR 94528 A 19940119
Cited Patents: EP 528730
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2715256	A1		31	H04L-009/12	
WO 9520280	A1	F	32	H04L-009/08	

Designated States (National): JP KR NO
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE

EP 740870	A1	F	31	H04L-009/08	Based on patent WO 9520280

Designated States (Regional): GB NL SE

US 5615265	A		11	H04N-007/167	
EP 740870	B1	F		H04L-009/08	Based on patent WO 9520280

Designated States (Regional): GB NL SE

Abstract (Basic): FR 2715256 A

The method includes assigning a specific control word (MCSi) acting as an encryption key for each transmitted programme (Pi) derived from a common encryption key (MCR) with diversification parameters (PDi). Each program is scrambled using its own key. Right of access is checked by two-part messages in which the first part (MCTAC) is common to all programmes and contains an operator identifier (ID) and control common encryption device (CMCR).

The second part contains the information specific to each program (MCTASi). These messages contain the access conditions (CAi) for different programmes (CAi) chosen by the same operator, the diversification parameters and a cryptographic check element (RCi). This guarantees the integrity of the complete message formed by the first common part and the second specific part.

USE/ADVANTAGE - E.g. radio, data transmission etc. Guarantees access to authorised users only. Reduced bit rate requirement for access control messages.

Dwg.1/6

Title Terms: CONDITION; PROGRAMME; ACCESS; METHOD; TELEVISION; BROADCAST; CHECK; USER; ACCESS; STATUS; MESSAGE; FIRST; PART; CONTAIN; PUBLIC; KEY; SECOND; PART; PROGRAMME; SPECIFIC; ENCRYPTION; INFORMATION
Derwent Class: W01; W02
International Patent Class (Main): H04L-009/08; H04L-009/12; H04N-007/167
International Patent Class (Additional): H04K-001/00; H04N-007/16
File Segment: EPI

11/5/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012348070 **Image available**
WPI Acc No: 1999-154177/ **199913**
Related WPI Acc No: 1996-465320; 1997-363998; 1998-363180; 1999-154174; 1999-154175; 1999-154176; 1999-154178; 1999-154179; 1999-181268; 1999-243551; 2002-060946; 2002-499082; 2002-705909; 2002-722051; 2002-722052; 2003-677663; 2003-898213; 2004-155029; 2004-478232; 2004-579235; 2004-623798
XRPX Acc No: N99-111142

Method for authenticating source of information in cable television **system**

Patent Assignee: SCIENTIFIC-ATLANTA INC (SCAT)
Inventor: AKINS G L; BANKER R O; PALGON M S; PINDER H G; WASILEWSKI A J
Number of Countries: 081 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9907149	A1	19990211	WO 98US16040	A	19980731	199913	B
AU 9887642	A	19990222	AU 9887642	A	19980731	199927	
EP 1013091	A1	20000628	EP 98939155	A	19980731	200035	
			WO 98US16040	A	19980731		
BR 9815606	A	20020122	BR 9815606	A	19980731	200216	
			WO 98US16040	A	19980731		
EP 1189439	A2	20020320	EP 98939155	A	19980731	200227	
			EP 2001126558	A	19980731		
EP 1013091	B1	20020918	EP 98939155	A	19980731	200269	
			WO 98US16040	A	19980731		
			EP 2001126558	A	19980731		
DE 69808113	E	20021024	DE 98608113	A	19980731	200278	
			EP 98939155	A	19980731		
			WO 98US16040	A	19980731		
JP 2003521718	W	20030715	WO 98US16040	A	19980731	200347	
			JP 2000505743	A	19980731		

Priority Applications (No Type Date): US 98127152 A 19980731; US 9754575 P 19970801
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9907149	A1	E	109	H04N-007/16	
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW					
AU 9887642	A				Based on patent WO 9907149
EP 1013091	A1	E			Based on patent WO 9907149
Designated States (Regional): DE FR GB IT NL					
BR 9815606	A				Based on patent WO 9907149
EP 1189439	A2	E			Div ex application EP 98939155 Div ex patent EP 1013091
Designated States (Regional): DE FR GB IT NL					
EP 1013091	B1	E		H04N-007/16	Related to application EP 2001126558 Related to patent EP 1189439 Based on patent WO 9907149
Designated States (Regional): DE FR GB IT NL					
DE 69808113	E			H04N-007/16	Based on patent EP 1013091 Based on patent WO 9907149
JP 2003521718	W		127	G09C-001/00	Based on patent WO 9907149

Abstract (Basic): WO 9907149 A1

NOVELTY - The programs received by **set top** units are decrypted using **public** or private **keys** provided by service providers or central authorization agents. Keys used by **set top** boxes (113) for selective decryption are public or private in nature and can be reassigned at different times to provide a **cable television** system

with minimal piracy.

DETAILED DESCRIPTION - The **cable television** system uses a head end from which service programs are broadcast and several **set top** units for receiving the programs and selectively decrypting them for display to system subscribers.

USE - For protecting information and more particularly systems for protecting information that is transmitted using wired or wireless medium against unauthorized access.

ADVANTAGE - Provides access restrictions which are both more secure and more flexible than those in conventional systems.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of a **conditional access** system.

set top box (113)

pp; 109 DwgNo 1/29

Title Terms: METHOD; AUTHENTICITY; SOURCE; INFORMATION; CABLE; TELEVISION; SYSTEM

Derwent Class: P85; W02

International Patent Class (Main): G09C-001/00; H04N-007/16

International Patent Class (Additional): H04L-009/08; H04N-007/10; H04N-007/167

File Segment: EPI; EngPI

11/5/14 (Item 14 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012240109 **Image available**

WPI Acc No: 1999-046217/ **199904**

XRPX Acc No: N99-033717

Global conditional access **system for broadcast services - includes authentication of selected list provided using** public key **and decrypting message using second private key stored in smart card**

Patent Assignee: THOMSON CONSUMER ELECTRONICS INC (THOH); THOMSON MULTIMEDIA INC (THOH); THOMSON CONSUMER ELECTRONICS SA (THOH)

Inventor: ESKICIOGLU A M; ESKICIOGLU A

Number of Countries: 082 Number of Patents: 010

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9856180	A1	19981210	WO 98US11634	A	19980605	199904	B
AU 9878189	A	19981221	AU 9878189	A	19980605	199919	
EP 988754	A1	20000329	EP 98926327	A	19980605	200020	
			WO 98US11634	A	19980605		
BR 9809917	A	20000801	BR 989917	A	19980605	200043	
			WO 98US11634	A	19980605		
CN 1265807	A	20000906	CN 98807914	A	19980605	200065	
MX 9911218	A1	20000601	MX 9911218	A	19991203	200133	
KR 2001013260	A	20010226	KR 99711252	A	19991201	200154	
AU 740825	B	20011115	AU 9878189	A	19980605	200202	
JP 2002503422	W	20020129	WO 98US11634	A	19980605	200211	
			JP 99502921	A	19980605		
KR 426740	B	20040408	WO 98US11634	A	19980605	200451	
			KR 99711252	A	19991201		

Priority Applications (No Type Date): US 9748852 P 19970606

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9856180	A1	E	29	H04N-007/167	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9878189	A		H04N-007/167	Based on patent WO 9856180
EP 988754	A1	E	H04N-007/167	Based on patent WO 9856180

Designated States (Regional): DE FR GB IT

BR 9809917	A		H04N-007/167	Based on patent WO 9856180

CN 1265807	A		H04N-007/167	
MX 9911218	A1		H04N-007/167	
KR 2001013260	A		H04N-007/167	
AU 740825	B		H04N-007/167	Previous Publ. patent AU 9878189 Based on patent WO 9856180
JP 2002503422	W	31	H04N-007/167	Based on patent WO 9856180
KR 426740	B		H04N-007/167	Previous Publ. patent KR 2001013260 Based on patent WO 9856180

Abstract (Basic): WO 9856180 A

A **conditional access** system includes a **set - top** box (400) having a smart card (420) coupled to a card reader and communicating with a billing centre (700) and also to many service providers (600) and to an electronic programme guide (580). The smart card could be integrated into the box for digital TV and lists of events from service providers could be accessed through the programme guide having a unique digitally signed and encrypted message associated with each event.

After selection of a desired event from the programme guide, the corresponding digitally signed message is downloaded into the **set - top** box and the guide must be authenticated to ensure the message was received from the desired provider. Authentication involves decrypting the digital signal in the **set - top** box using the **public key** of the provider and requires a pre-existing agreement between the provider source and the manufacturer of the **set - top** box. After authentication, the message is decrypted in the **set - top** box and data of the channel identification, the date and time are used to update the user account.

USE - Providing of **conditional access** to **set - top** box of digital TV receiving digital streams from various sources

ADVANTAGE - Compensation of manufacturer for use of hardware to access selected service provider

Dwg.3/4

Title Terms: GLOBE; CONDITION; ACCESS; SYSTEM; BROADCAST; SERVICE; AUTHENTICITY; SELECT; LIST; PUBLIC; KEY; MESSAGE; SECOND; PRIVATE; KEY; STORAGE; SMART; CARD

Derwent Class: P85; T01; T04; W01; W02; W03

International Patent Class (Main): H04N-007/167

International Patent Class (Additional): C07D-235/08; G09C-001/00; H04H-001/00; H04L-009/08; H04L-009/32; H04N-005/00; H04N-007/16

File Segment: EPI; EngPI

11/5/15 (Item 15 from file: 350)

011536582 **Image available**

WPI Acc No: 1997-513063/ **199747**

XRPX Acc No: N97-427073

Secure communication method especially for pay TV system - generating and transferring random key in encrypted message and decrypting message using corresponding secret key to obtain random key

Patent Assignee: DIGCO BV (DIGC-N); IRDETO ACCESS BV (IRDE-N); DAVIES D W (DAVI-I); GLASSPOOL A (GLAS-I); RIX S P A (RIXS-I)

Inventor: DAVIES D W; GLASSPOOL A; RIX S P A

Number of Countries: 079 Number of Patents: 014

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9738530	A1	19971016	WO 97EP1557	A	19970321	199747	B
ZA 9702786	A	19971231	ZA 972786	A	19970402	199807	
AU 9725063	A	19971029	AU 9725063	A	19970321	199810	
EP 891670	A1	19990120	EP 97916402	A	19970321	199908	
			WO 97EP1557	A	19970321		
CN 1215528	A	19990428	CN 97193565	A	19970321	199935	
BR 9708500	A	19990803	BR 978500	A	19970321	199952	
			WO 97EP1557	A	19970321		
EP 891670	B1	20000614	EP 97916402	A	19970321	200033	
			WO 97EP1557	A	19970321		

TW 369778	A	19990911	TW 97109713	A	19970710	200035
JP 2000508482	W	20000704	JP 97535793	A	19970321	200037
			WO 97EP1557	A	19970321	
DE 69702310	E	20000720	DE 602310	A	19970321	200041
			EP 97916402	A	19970321	
			WO 97EP1557	A	19970321	
MX 9808217	A1	19990401	MX 988217	A	19981005	200055
ES 2149585	T3	20001101	EP 97916402	A	19970321	200062
US 6385317	B1	20020507	WO 97EP1557	A	19970321	200235
			US 99155782	A	19990402	
US 20020126844	A1	20020912	US 99155782	A	19990402	200262
			US 2002101122	A	20020318	

Priority Applications (No Type Date): EP 96200907 A 19960403
Cited Patents: 1.Jnl.Ref; EP 428252; EP 658054; US 5029207
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9738530	A1	E	13	H04N-007/16	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN YU
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

ZA 9702786	A	12	H04N-000/00	
AU 9725063	A			Based on patent WO 9738530
EP 891670	A1	E		Based on patent WO 9738530

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

BR 9708500	A			Based on patent WO 9738530
EP 891670	B1	E	H04N-007/16	Based on patent WO 9738530

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

TW 369778	A		H04N-007/16	
JP 2000508482	W	20	H04N-007/167	Based on patent WO 9738530
DE 69702310	E		H04N-007/16	Based on patent EP 891670
				Based on patent WO 9738530
MX 9808217	A1		H04N-007/16	
ES 2149585	T3		H04N-007/16	Based on patent EP 891670
US 6385317	B1		H04H-009/00	Based on patent WO 9738530
US 20020126844	A1		H04N-007/167	Cont of application US 99155782
				Cont of patent US 6385317

Abstract (Basic): WO 9738530 A

The method involves generating a random key (Ci) by a **conditional access** module (CAM) used in a pay TV system and transferring the key to a smart card. The key is encrypted in a first message using a **public key** . The smart card decrypts the encrypted message using a corresponding secret key to obtain the random key.

The random key is used to encrypt and decrypt transmissions between the devices. Preferably, after decryption of the message, the smart card returns the random key in a second encrypted message with an authentication to the **conditional access** module.

ADVANTAGE - Prevents switching between authorised and unauthorised devices.

Dwg.2/2

Title Terms: SECURE; COMMUNICATE; METHOD; PAY; TELEVISION; SYSTEM; GENERATE ; TRANSFER; RANDOM; KEY; ENCRYPTION; MESSAGE; MESSAGE; CORRESPOND; SECRET ; KEY; OBTAIN; RANDOM; KEY
Derwent Class: P85; W02; W03
International Patent Class (Main): H04H-009/00; H04N-000/00; H04N-007/16; H04N-007/167
International Patent Class (Additional): G09C-000/00; H04K-000/00; H04L-009/00
File Segment: EPI; EngPI

11/5/16 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010792383 **Image available**
WPI Acc No: 1996-289336/ **199630**
Related WPI Acc No: 1995-353054; 1996-173232; 1996-211260; 1996-261833; 2000-012066; 2000-115324; 2000-474732; 2000-654981; 2002-259220; 2004-466660
XRPX Acc No: N96-242825

Crypt key system esp. for copyright protection or management in television broadcasting or online database - uses secret key and public key **encryption methods as well as digital signature with crypt keys supplied through broadcast being optionally encrypted**

Patent Assignee: MITSUBISHI CORP (MITS)
Inventor: SAITO M

Number of Countries: 005 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 719045	A2	19960626	EP 95119605	A	19951213	199630	B
EP 719045	A3	19961016	EP 95119605	A	19951213	199648	
JP 8288940	A	19961101	JP 95346095	A	19951211	199703	
US 5740246	A	19980414	US 95573958	A	19951213	199822	
US 6182218	B1	20010130	US 95573958	A	19951213	200108	
			US 97881533	A	19970624		
US 20020052850	A1	20020502	US 95549270	A	19951027	200234	
			US 95573958	A	19951213		
			US 97868488	A	19970603		
			US 200113507	A	20011213		
US 6424715	B1	20020723	US 95549270	A	19951027	200254	
			US 95573958	A	19951213		
			US 97868488	A	19970603		
EP 719045	B1	20031029	EP 95119605	A	19951213	200379	
DE 69532028	E	20031204	DE 95632028	A	19951213	200404	
			EP 95119605	A	19951213		

Priority Applications (No Type Date): JP 94309292 A 19941213; JP 94264200 A 19941027; JP 94299835 A 19941202
Cited Patents: No-SR.Pub; 1.Jnl.Ref; EP 438154; EP 450841; EP 506435
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 719045	A2	E	21	H04N-007/167	
Designated States (Regional): DE FR GB					
EP 719045	A3			H04N-007/167	
JP 8288940	A		15	H04L-009/08	
US 5740246	A		18	H04N-007/167	
US 6182218	B1			H04L-009/00	CIP of application US 95573958 CIP of patent US 5740246
US 20020052850	A1			G06F-017/60	CIP of application US 95549270 CIP of application US 95573958 Div ex application US 97868488
US 6424715	B1			H04L-009/32	CIP of application US 95549270 CIP of application US 95573958 CIP of patent US 5740246
EP 719045	B1	E		H04N-007/167	
Designated States (Regional): DE FR GB					
DE 69532028	E			H04N-007/167	Based on patent EP 719045

Abstract (Basic): EP 719045 A

The crypt key system includes a database (12) which is connected to a broadcasting system (11) and a charging centre (13). A user terminal (18) receives (14) the broadcast information and directly communicates (15) with the database. Communication can be via direct links or intermediate storage e.g. floppy disc.

The database prepares a **public key** and supplies it to the broadcast station which sends it by teletext. The key can include a digital signature. Users can encrypt the **public key** with their secret key and send it to the database. This decodes it with a private key and encrypts the data which is then sent to the user who is able to decrypt it.

ADVANTAGE - For pay-per-view and video-on-demand systems. Also for online database system or electronic market. Defines concrete structure for applying the crypt key system to public access information systems.
Dwg.2/5

Title Terms: CRYPT; KEY; SYSTEM; PROTECT; MANAGEMENT; TELEVISION; BROADCAST ; DATABASE; SECRET; KEY; PUBLIC; KEY; ENCRYPTION; METHOD; WELL; DIGITAL; SIGNATURE; CRYPT; KEY; SUPPLY; THROUGH; BROADCAST; OPTION; ENCRYPTION
Index Terms/Additional Words: **CATV** ; CABLE; TV; MULTIMEDIA; LAN; WAN; INTERNET
Derwent Class: P85; T01; W01; W02; W03
International Patent Class (Main): G06F-017/60; H04L-009/00; H04L-009/08; H04L-009/32; H04N-007/167
International Patent Class (Additional): G06F-011/34; G06F-012/16; G06F-015/00; G09C-001/00; H04H-001/00; H04L-009/30
File Segment: EPI; EngPI

11/5/17 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010764879 **Image available**
WPI Acc No: 1996-261833/ **199627**
Related WPI Acc No: 1995-353054; 1996-173232; 1996-211260; 1996-289336; 2000-012066; 2000-115324; 2000-474732; 2000-654981; 2002-259220; 2004-466660
XRPX Acc No: N96-220230

Data copyright management appts. for computer, television set, set - top **box, digital VTR, digital video disk recorder, DAT or personal digital assistant - stores copyright management program in ROM and if received externally, stores in EEPROM**

Patent Assignee: MITSUBISHI CORP (MITS)
Inventor: MOMIKI S; SAITO M
Number of Countries: 005 Number of Patents: 015
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 715241	A2	19960605	EP 95116615	A	19951021	199627	B
JP 8287014	A	19961101	JP 95280984	A	19951027	199703	
US 5867579	A	19990202	US 95549270	A	19951027	199912	
			US 97779751	A	19970110		
US 6128605	A	20001003	US 95549270	A	19951027	200050	
			US 97882909	A	19970626		
US 20010013021	A1	20010809	US 95549270	A	19951027	200147	
			US 97779751	A	19970110		
			US 9897877	A	19980615		
			US 2001768287	A	20010125		
US 20020052850	A1	20020502	US 95549270	A	19951027	200234	
			US 95573958	A	19951213		
			US 97868488	A	19970603		
			US 200113507	A	20011213		
US 20020059238	A1	20020516	US 95536747	A	19950929	200237	
			US 95549270	A	19951027		
			US 97825868	A	19970402		
			US 99362955	A	19990730		
			US 2001985376	A	20011102		
US 6408390	B1	20020618	US 95549270	A	19951027	200244	
			US 98781679	A	19980724		
			US 99375000	A	19990816		
US 6424715	B1	20020723	US 95549270	A	19951027	200254	
			US 95573958	A	19951213		
			US 97868488	A	19970603		
US 20020112173	A1	20020815	US 95549270	A	19951027	200256	
			US 97799751	A	19970213		
			US 9897877	A	19980615		
			US 2001768287	A	20010125		
			US 2002105262	A	20020326		
US 6438694	B2	20020820	US 95549270	A	19951027	200257	
			US 97779751	A	19970110		

			US 9897877	A	19980615	
			US 2001768287	A	20010125	
EP 715241	B1	20040114	EP 95116615	A	19951021	200406
DE 69532434	E	20040219	DE 95632434	A	19951021	200419
			EP 95116615	A	19951021	
US 6741991	B2	20040525	US 95536747	A	19950929	200435
			US 95549270	A	19951027	
			US 97825868	A	19970402	
			US 99362955	A	19990730	
			US 2001985376	A	20011102	
US 6789197	B1	20040907	US 95549270	A	19951027	200459
			US 97882909	A	19970626	
			US 2000676495	A	20001002	

Priority Applications (No Type Date): JP 94299835 A 19941202; JP 94264200 A 19941027; JP 94309292 A 19941213; JP 94237673 A 19940930; JP 94264199 A 19941027; JP 94269959 A 19941102

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 715241	A2	E	34	G06F-001/00	
Designated States (Regional): DE FR GB					
JP 8287014	A		24	G06F-015/00	
US 5867579	A			H04K-001/00	Div ex application US 95549270
US 6128605	A			H04L-009/00	Cont of application US 95549270
US 20010013021	A1			H04L-009/00	Div ex application US 95549270 Div ex application US 97779751 Cont of application US 9897877 Div ex patent US 5867579
US 20020052850	A1			G06F-017/60	CIP of application US 95549270 CIP of application US 95573958 Div ex application US 97868488
US 20020059238	A1			G06F-007/00	CIP of application US 95536747 CIP of application US 95549270 Div ex application US 97825868 Cont of application US 99362955
US 6408390	B1			G06F-011/30	Div ex application US 95549270 Cont of application US 98781679
US 6424715	B1			H04L-009/32	CIP of application US 95549270 CIP of application US 95573958 CIP of patent US 5740246
US 20020112173	A1			H04L-009/32	Div ex application US 95549270 Div ex application US 97799751 Cont of application US 9897877 Cont of application US 2001768287
US 6438694	B2			G06F-009/00	Div ex application US 95549270 Div ex application US 97779751 Cont of application US 9897877 Div ex patent US 5867579
EP 715241	B1	E		G06F-001/00	
Designated States (Regional): DE FR GB					
DE 69532434	E			G06F-001/00	Based on patent EP 715241
US 6741991	B2			G06F-017/30	CIP of application US 95536747 CIP of application US 95549270 Div ex application US 97825868 Cont of application US 99362955 Div ex patent US 6002772 CIP of patent US 6069952
US 6789197	B1			H04L-009/00	Cont of application US 95549270 Cont of application US 97882909 Cont of patent US 6128605

Abstract (Basic): EP 715241 A

A CPU, a read-only semiconductor memory, an EEPROM, a read-write memory are connected to a CPU bus. A system bus terminal is connected to the CPU bus. A data copyright management. system program, a copyright management. program and user information are stored in the read-only memory.

A second private-key, a permit key, a second secret key, a

copyright management are provided. Program and copyright information are stored in the EEPROM. Two **public keys** , a private key and a encryption key are transmitted to the read-write memory during operation.

ADVANTAGE - Data copyright management. appts. as multiprocessor configuration utilising SCSI bus or PCI bus is accomplished.

Dwg.3/15

Title Terms: DATA; MANAGEMENT; APPARATUS; COMPUTER; TELEVISION; SET; SET; TOP; BOX; DIGITAL; VTR; DIGITAL; VIDEO; DISC; RECORD; DAT; PERSON; DIGITAL; ASSIST; STORAGE; MANAGEMENT; PROGRAM; ROM; RECEIVE; EXTERNAL; STORAGE; EEPROM

Derwent Class: P85; T01; W01; W02; W03

International Patent Class (Main): G06F-001/00; G06F-007/00; G06F-009/00; G06F-011/30; G06F-015/00; G06F-017/30; G06F-017/60; H04K-001/00; H04L-009/00; H04L-009/32

International Patent Class (Additional): G06F-011/34; G06F-012/16; G09C-001/00; H04L-009/08; H04L-009/10; H04N-007/15; H04N-007/167

File Segment: EPI; EngPI